

**BEFORE THE  
FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON, D.C. 20554**

In the Matter of	)	
	)	
Digital Output Protection Technology	)	
and Recording Method Certifications:	)	MB Docket No. 04-59
	)	
SmartRight	)	
	)	

**REPLY OF SMARTRIGHT APPLICANTS TO THE OPPOSITION  
OF THE MOTION PICTURE ASSOCIATION OF AMERICA, INC., ET AL**

David H. Arland  
Vice President, U.S. Corporate Communications  
and Government Relations  
Thomson Inc.  
P.O. Box 1976, INH-430  
Indianapolis, IN 46206-1976  
(317) 587-4832

April 16, 2004

## TABLE OF CONTENTS

I.	INTRODUCTION AND SUMMARY .....	2
II.	SMARTRIGHT WILL IMPOSE REASONABLE AND AFFIRMATIVE CONSTRAINTS ON REDISTRIBUTION OF “FLAGGED” DIGITAL BROADCAST CONTENT .....	5
A.	For Purposes of Approval Pursuant to the Commission’s Interim Procedures, SmartRight Will Assert Proximity Controls For All Marked and Unscreened Content, Permitting Redistribution Only Within A Localized Environment .....	7
B.	For Purposes of Approval Pursuant To The Commission’s Interim Procedures, SmartRight Will Require Physical Propagation of the Personal Private Network .....	9
III.	SMARTRIGHT WILL AMEND ITS COMPLIANCE RULES TO ASSERT UPSTREAM CONTROLS OVER DOWNSTREAM HDCP FUNCTIONS .....	10
IV.	SMARTRIGHT PROVIDES FOR MEANINGFUL CONTENT OWNER PARTICIPATION AND ENFORCEMENT .....	11
V.	SMARTRIGHT PROVIDES FOR EFFECTIVE CHANGE MANAGEMENT PROCEDURES AND MEANINGFUL CONTENT OWNER PARTICIPATION .....	14
VI.	THE TERMS OF THE SMARTRIGHT ADOPTER AGREEMENT WILL APPLY TO ALL EQUIPMENT MANUFACTURERS, AND NO OBLIGATIONS ARE PLACED ON CONTENT OWNERS, BROADCASTERS, OR CONSUMERS BY VIRTUE OF DISTRIBUTING BROADCAST FLAG CONTENT .....	15
VII.	CONCLUSION.....	16

APPENDIX A – SMARTRIGHT ADOPTER AGREEMENT

APPENDIX B – SMARTRIGHT CONTENT PARTICIPANT AGREEMENT

**BEFORE THE  
FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON, D.C. 20554**

In the Matter of	)	
	)	
Digital Output Protection Technology	)	
and Recording Method Certifications:	)	MB Docket No. 04-59
	)	
SmartRight	)	
	)	

**REPLY OF SMARTRIGHT APPLICANTS TO THE OPPOSITION  
OF THE MOTION PICTURE ASSOCIATION OF AMERICA, INC., ET AL**

Thomson Inc. (“Thomson”), on behalf of itself and its SmartRight partners (collectively, “SmartRight Applicants”),<sup>1</sup> hereby replies to the Opposition filed by the Motion Picture Association of America, Inc. and its member studios (collectively, the “MPAA Parties”)<sup>2</sup> to the Certification of SmartRight for approval as a digital output protection technology and recording method.<sup>3</sup> This Reply provides further details and clarifications regarding both the operation of the SmartRight system and the rights of content participants directly responsive to each concern

---

<sup>1</sup> SmartRight’s partners include: Axalto, Gemplus S.A., Micronas, Nagravision S.A., Pioneer Corporation, SCM Microsystems, and ST Microelectronics N.V. and Thomson.

<sup>2</sup> *In the Matter of Digital Output Protection Technology and Recording Method Certifications: SmartRight*, Opposition To The Application of SmartRight by the Motion Picture Association of America Inc., Metro-Goldwyn-Mayer Studios Inc., Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corporation, Universal City Studios LLLP, The Walt Disney Company, and Warner Bros. Entertainment Inc., MB Docket No. 04-59 (April 6, 2004) (“*MPAA Parties’ Opposition*”).

<sup>3</sup> *In the Matter of Digital Output Protection Technology and Recording Method Certifications: SmartRight*, MB Docket No. 04-59 (March 1, 2004) (“*SmartRight Certification*”); Certifications for Digital Output Protection Technologies and Recording Methods to be Used in Covered Demodulator Products: Commission Announces Certifications Received and Opens Window for Comments and Oppositions, *Public Notice*, DA 04-715 (*rel.* March 17, 2004).

raised by the MPAA Parties. The SmartRight Certification, buttressed by the explanatory information contained in this Reply, merits Commission approval.

## **I. INTRODUCTION AND SUMMARY**

The MPAA Parties' Opposition raises two distinct categories of concerns regarding the SmartRight Certification. The first encompasses a number of issues, including: upstream control over downstream HDCP functions; equal applicability of Compliance and Robustness Rules to all adopters, including equipment manufacturers that also are technology proponents; insertion of the Broadcast Flag by content providers and broadcasters not triggering intellectual property obligations, etc., which are common, at least in part, to all of the MPAA Parties' filings pertinent to certifications of digital broadcast content protection technologies, including those supported by the MPAA Parties. The second category of concerns, apparently sparking the MPAA Parties' opposition rather than conditional support, relate to two broad issues: (1) the potential for SmartRight to provide for "remote access" to digital broadcast content redistributed over the Internet beyond a "localized environment" and the manner in which proximity controls could constrain such redistribution; and (2) the role of content participants in change management procedures and the initiation and enforcement of revocation and renewal.

This Reply addresses the first category of concerns, those also extending to MPAA-supported technologies, principally by providing the specific assurances the MPAA Parties sought in their Opposition. In some instances, changes to the Compliance Rules in the SmartRight Adopter Agreement were made to accommodate these concerns. In other instances, the Reply provides clarification explicitly eliminating the problem identified by the MPAA Parties.

The SmartRight Applicants believe that a common thread linking the second category of concerns was insufficient specific information in the SmartRight Certification to provide the MPAA Parties with assurances that deployment of an FCC-approved SmartRight system would not harm content producers' core interests in protecting their intellectual property and maintaining the broadcasting business model.

This Reply provides abundant additional information that should allay both principal concerns.

In this filing, SmartRight describes in detail specific proximity controls it is prepared to activate in an initial implementation of an FCC-approved system, that would have the effect of limiting SmartRight to the home networking environment. This approach provides an interim engineering solution directly responsive to the localization issue raised in the MPAA Parties' Opposition.<sup>4</sup> The SmartRight Applicants note that activation of such stringent proximity controls is not required by the scope of redistribution described in the Commission's November 4, 2003 *Broadcast Flag Report and Order*.<sup>5</sup> Moreover, these proximity controls constrain inherent competitive and pro-consumer advantages of SmartRight's authorized domain system. The SmartRight Applicants are willing to adopt tight proximity controls for this initial implementation in order to preserve the Commission's ability to decide the important related policy issues currently pending before it in the *Broadcast Flag FNPRM* without having to

---

<sup>4</sup> The MPAA also is raising this concern in connection with the *Broadcast Flag FNPRM*. See March 19, 2004 Letter from Fritz E. Attaway, Motion Picture Association of America, to Marlene Dortch in MB Docket No. 02-230, Power Point Presentation.

<sup>5</sup> See *In the Matter of Digital Broadcast Content Protection*, MB Docket No. 02-230, *Report and Order and Further Notice of Proposed Rulemaking*, 18 FCC Rcd 23550 (2003) ("*Broadcast Flag Report and Order*" and "*Broadcast Flag FNPRM*" as appropriate) at ¶ 63 ("In general, we believe that a flag-based system should prevent indiscriminate redistribution of digital broadcast content, however, we do not wish to foreclose use of the Internet to send digital broadcast content where robust security can adequately protect the content and the redistribution is tailored in nature.")

confront changed realities “in the field.” The proximity controls can then be maintained, relaxed or eliminated to comply with the Commission’s determination.

Additionally, the SmartRight Applicants are including with this Reply a Content Participant Agreement describing in detail the extensive and meaningful participation afforded to SmartRight Content Participants in changes, including those that could potentially affect the security or integrity of the SmartRight system, as well as revocation and renewal. To ensure consistency with the new Content Participant Agreement, the SmartRight Applicants also are submitting an amended version of the SmartRight License Agreement (originally included as Appendix A to the SmartRight Certification).<sup>6</sup> The revised SmartRight Adopter Agreement also incorporates changes discussed elsewhere in this Reply.

The SmartRight Applicants believe that the information provided in this Reply should enable the MPAA Parties to support Commission approval of the SmartRight system. Such approval would advance the Commission’s goal of fostering a competitive digital broadcast content protection technology marketplace. It would permit deployment of an innovative system offering both greater security and greater consumer use and enjoyment of DTV than other candidate systems for FCC approval.

---

<sup>6</sup> The amended SmartRight License Agreement, retitled “SmartRight Adopter Agreement,” is attached as Appendix A to this Reply (“*SmartRight Adopter Agreement*”).

## **II. SMARTRIGHT WILL IMPOSE REASONABLE AND AFFIRMATIVE CONSTRAINTS ON REDISTRIBUTION OF “FLAGGED” DIGITAL BROADCAST CONTENT**

The MPAA Parties seek clarification regarding SmartRight’s ability to “impose reasonable and affirmative constraints on redistribution of content,” specifically regarding: (1) the extent to which SmartRight’s proximity controls will limit the redistribution of protected content; and (2) the methods by which propagation of the SmartRight Personal Private Network (“PPN”) is established and managed, focusing especially on the instance when a remote Display Device attempts to join the PPN across the Internet.<sup>7</sup> The MPAA Parties request this information to establish whether SmartRight “achieves the proximity controls necessary to protect Marked and Unscreened Content against unauthorized redistribution.”<sup>8</sup>

As discussed in its Certification, the SmartRight system offers proximity controls which, once asserted, control the redistribution over the Internet of SmartRight-protected content between remote locations within the same PPN, based upon the geographic proximity of those locations.<sup>9</sup> In fact, SmartRight’s proximity controls, like the entire system, are remarkably flexible, and can allow for either greater or lesser (though always secure) redistribution of protected content via the Internet depending upon whether or not they are invoked and how they are set. To wit, SmartRight’s proximity controls, if asserted liberally or not asserted, will permit secure and discriminate transmissions of protected content over an IP network or the Internet to virtually any remotely-located device within a consumer’s Personal Private Network.

---

<sup>7</sup> *MPAA Parties’ Opposition* at 3-4.

<sup>8</sup> *MPAA Parties’ Opposition* at 4.

<sup>9</sup> *See SmartRight Certification* at § 5.4.

Alternatively, if more strictly set, redistribution can be constrained within a tightly-defined physical environment, such as a wired or wireless home network.

SmartRight Applicants agree with the MPAA Parties that the question of whether and how to employ proximity limits – *i.e.*, how or even whether to define the “personal digital network environment” – is a question pending before the Commission in its *Broadcast Flag FNPRM*.<sup>10</sup> On the one hand, the Commission’s *Broadcast Flag Report and Order* establishes, at least for technologies approved under its interim process rules, a scope of redistribution that would appear to countenance SmartRight’s use of very permissive proximity controls or perhaps no proximity controls – thus permitting consumers to engage in lawful, secure, and discriminating transmissions of protected content over the Internet.<sup>11</sup> On other hand, SmartRight Applicants are sensitive to content owners’ concerns that, during this interim period, the Commission not approve technologies that effectively define “remote access” in so broad a manner as to prejudge the outcome of issues raised in the *Broadcast Flag FNPRM* or, more importantly, jeopardize the fundamental broadcast model.<sup>12</sup>

To bridge this gap, and in the interest of ensuring the development of a robustly competitive market for digital broadcast content protection technologies, SmartRight Applicants urge the Commission to consider a short-term solution which we believe is both achievable and would not prejudge the Commission’s final decision regarding whether and to what extent “remote access” will be permitted. Under this proposal, SmartRight would receive initial approval under the Commission’s interim process rules on the condition that proximity controls are invoked which effectively constrain redistribution of Marked and Unscreened Content to

---

<sup>10</sup> See MPAA Parties’ *Opposition* at 5, n.2; See *Broadcast Flag FNPRM* at ¶ 63.

<sup>11</sup> See *Broadcast Flag Report and Order* at ¶¶ 10, 63.

<sup>12</sup> See MPAA Parties’ *Opposition* at 5, n.2.



within a localized environment (*i.e.*, a home network and its immediate environs) and requiring physical propagation of a SmartRight PPN.

Such approval would not, however, prejudice SmartRight Applicants' (and others') advocating in support of the Commission's adopting permanent approval criteria that permit more relaxed (but no less secure) implementation of SmartRight, both with respect to content redistribution and PPN propagation, to permit greater use and enjoyment of DTV by consumers. Indeed, if the Commission ultimately concludes that such remote access can and/or should be permitted by an approved technology, SmartRight's proximity controls can be relaxed or removed to comport with the Commission's decision. Such compliance should not trigger a new approval process.

**A. For Purposes of Approval Pursuant to the Commission's Interim Procedures, SmartRight Will Assert Proximity Controls For All Marked and Unscreened Content, Permitting Redistribution Only Within A Localized Environment**

SmartRight's proximity controls, which use a balanced analysis of the number of routers, and the latency time of communication, will block the transfer of protected content over a Wide Area Network, based upon parameters that should be acceptable to the owners of the content being transferred.

In deference to the MPAA Parties' concerns regarding the need to require "localization" pending the Commission's adoption of permanent selection criteria defining parameters for "remote access," if approved pursuant to the Commission's interim process, SmartRight will assert proximity controls for all Marked and Unscreened Content using the following parameters:

- 1) Time-To-Live (TTL): The TTL (the number of router hops a packet takes between the source device and the sink device) will be set to 3.<sup>13</sup>
- 2) Round-Trip-Time (RTT): The maximum RTT (the time it takes to send a packet to a remote host and receive a response) will be set, in consultation with content owners, at a value that will restrict redistribution to the localized environment – i.e., within the home network.<sup>14</sup>
- 3) SmartRight will detect proximity controls every 60 seconds.

Based on these parameters, content received within a SmartRight PPN would be freely copiable within the consumers' PPN, but constrained from redistribution over the Internet beyond the localized environment of that PPN. Notably, under such proximity control settings, the consumer would not lose the ability to copy SmartRight-protected content onto recordable media for viewing either on remote devices within that same consumer's PPN,<sup>15</sup> or on devices employing any other FCC-approved technology.

---

<sup>13</sup> This TTL value is consistent with that reflected in the work plan for DTCP-IP referenced in MPAA's Response to DTLA's Certification of DTCP. *See* Response of MPAA to the DTCP Certification, MB Docket No. 04-64 (April 6, 2004) ("*MPAA DTCP Response*") at 3.

<sup>14</sup> SmartRight Applicants will work with MPAA and its members to arrive at a mutually-acceptable RTT value that preserves consumers' ability to distribute protected content freely within the localized home network over wired and wireless connections. The appropriate value of the RTT for this application is a technically sophisticated question, as evidenced by the apparently extensive effort undertaken to address this issue in the DTCP-IP context. *See MPAA DTCP Response* at 3. Notably, a system's RTT value must take into account the architecture of that system. For instance, whereas link protection systems (such as DTCP) – which involve transmissions only between 2 devices over a wired connection – might be able to achieve effective localized redistribution of content based upon a shorter RTT, SmartRight's secure domain architecture – which involves multiple, successive (secure) transmissions between 2 or more devices using any number of *wired or wireless* connections – requires, to function meaningfully, a greater RTT limit in order to permit the free flow of protected over-the-air digital broadcast content within the localized environment.

<sup>15</sup> As discussed below, associating remotely-located devices to a PPN will require physical insertion of a SmartRight smart card.

**B. For Purposes of Approval Pursuant To The Commission's Interim Procedures, SmartRight Will Require Physical Propagation of the Personal Private Network**

As discussed in its Certification, the SmartRight system incorporates the capability to permit the consumer to include remotely-located SmartRight devices within his or her PPN.<sup>16</sup> The SmartRight system could be configured to propagate the PPN through an IP network, including over the Internet, and in that implementation would rely on appropriately-set proximity controls to ensure a reasonable degree of localization for protected content. The MPAA Parties, however, also have expressed concern about the impact of this approach on localization.

Again, recognizing the MPAA Parties' concerns that approval of such a propagation mechanism might prejudice the Commission's consideration of directly related pending issues in the *Broadcast Flag FNPRM*, for purposes of its authorization under the Commission's interim process rules, SmartRight is prepared to require only *physical* propagation of the PPN – with a limit of 10 Display Devices<sup>17</sup> – which involves physical insertion of an authorized smart card into the new Display Device.<sup>18</sup> The provisional exclusive reliance on physical propagation of the PPN should eliminate the MPAA Parties' concern with this SmartRight feature.

---

<sup>16</sup> See *SmartRight Certification* at § 8.2. A Terminal Module is contained in each Display Device. The Terminal Module contained in the last Display Device added to the PPN maintains the total count of display devices on the PPN. When that limit is reached, no more Display Devices may be added.

<sup>17</sup> In its Certification, it was indicated that SmartRight would limit the number of Display Devices to a reasonably-defined number. See *SmartRight Certification* at § 5.3. Based upon consultations with the content community since that time, SmartRight will set that limit at 10. Such a limit would permit, e.g., six Display Devices within the home, as well as one each in an office, summer home, car and boat. SmartRight imposes no limitation on the number of devices with reception or storage capability that can be attached to the PPN.

<sup>18</sup> Notably, because joining a device to an existing PPN, or even creating a new PPN does not require the consumer's connecting the device to a "back office" via the Internet or dialup for registration, there is no disclosure or exposure of any personally-identifiable information. See *SmartRight Certification* at § 8.2.

### **III. SMARTRIGHT WILL AMEND ITS COMPLIANCE RULES TO ASSERT UPSTREAM CONTROLS OVER DOWNSTREAM HDCP FUNCTIONS**

In its Opposition to the SmartRight Certification, the MPAA Parties indicate that SmartRight should assert an upstream control function to compensate for HDCP's inability to "assert control over the output of (or prevent the delivery of) Marked and Unscreened Content to an HDCP device, but can only signal upstream to the proposed technology when the HDCP function is actively engaged and able to deliver protected content."<sup>19</sup> The MPAA Parties articulate the identical concern regarding all the digital broadcast content protection technologies certified to the Commission that they did not oppose, except for CPRM (which has a compliance rule to address this problem).<sup>20</sup>

SmartRight Applicants recognize this anomaly of HDCP. The most appropriate approach to resolve this problem would be through a change in the HDCP Specification or Compliance Rules. In light of the time constraints associated with the approval process under Section 73.9008 of the FCC regulations, however, the SmartRight Applicants are willing to amend the SmartRight Compliance Rules in the following manner:

When passing Decrypted SmartRight content to an output protected by HDCP, a Presentation Device shall (a) carry any HDCP system Renewability Message delivered in association with such content to the HDCP Source function and (b) verify that the HDCP Source Function is engaged and able to deliver protected content, which means (i) HDCP encryption is operational on such output, (ii) processing of the valid received System Renewability Message associated with such content, if any, has occurred as defined in the HDCP Specification and (iii) there is no HDCP Display Device or Repeater on such output whose Key

---

<sup>19</sup> See *MPAA Parties' Opposition* at 7.

<sup>20</sup> *Id.* at 7; See Response of the MPAA Parties to the MagicGate Certifications, MB Docket Nos. 04-55, 04-56, 04-57, 04-58 (April 6, 2004) ("*MPAA MagicGate Response*") at 3-4; Response of the MPAA Parties to the Vidi Certification, MB Docket No. 04-60 (April 6, 2004) ("*MPAA Vidi Response*") at 3-4; Response of the MPAA Parties to the D-VHS Certification, MB Docket No. 04-68; (April 6, 2004) ("*MPAA D-VHS Response*") at 4-5; *MPAA DTCP Response* at 4-5.

Selection Vector is in such System Renewability Message. Capitalized terms used in the foregoing but not otherwise defined in the Specifications or the License shall have the meaning set forth in the HDCP Specification and HDCP License Agreement offered by Digital Content Protection, LLC.<sup>21</sup>

#### **IV. SMARTRIGHT PROVIDES FOR MEANINGFUL CONTENT OWNER PARTICIPATION AND ENFORCEMENT**

The MPAA Parties oppose the SmartRight Certification on the grounds that it does not provide content owners with adequate participation in the SmartRight revocation and renewal processes.<sup>22</sup> The MPAA Parties also request that the SmartRight Applicants address the systemic problem of the need for standardized revocation information to be embedded in the ATSC transport stream.<sup>23</sup>

At the outset, the SmartRight Applicants wish to underscore that the SmartRight Adopter Agreement grants full third-party beneficiary rights to all persons who distribute or transmit, or cause or authorize the distribution or transmission of Marked Content.<sup>24</sup> Thus, any content owner who invokes the Broadcast Flag has the automatic right to directly enforce the SmartRight Compliance Rules against equipment manufacturers. These third-party beneficiary rights are wholly independent of additional rights granted by the new Content Participant Agreement discussed in detail below.

In response to the MPAA Parties' concerns regarding revocation and renewal, as well as concerns regarding changes, SmartRight Applicants are filing with this Reply a Content

---

<sup>21</sup> This provision is patterned after the corresponding compliance rule in the CPRM license, evidently acceptable to MPAA. *See In the Matter of Digital Output Protection Technology and Recording Method Certifications: Content Protection Recordable Media for Video Content* ("CPRM"), MB Docket No. 04-62 (March 1, 2004), Appendix 1, "4C CPRM/CPPM License Agreement (including Compliance and Robustness Rules)," Exhibit C-3a at § 4.1.1.2.

<sup>22</sup> *See MPAA Parties' Opposition* at 8-9.

<sup>23</sup> *Id.* at 9.

<sup>24</sup> *See SmartRight Adopter Agreement* at § 10.4.

Participant Agreement, which is intended to allay these concerns.<sup>25</sup> This Content Participant Agreement confers specific additional rights on content providers. The SmartRight Applicants wish to make absolutely clear, however, that content providers or broadcasters are not *required* to sign the Content Participant Agreement in order for the SmartRight technology to be used to protect their content in the Broadcast Flag application.

The SmartRight Content Participant Agreement expressly provides for requests for revocation by Content Participants.<sup>26</sup> Content Participants may submit requests for revocation to the SmartRight Association, a separate, non-profit organization whose membership will include Content Participants, by submitting evidence of facts that satisfy one or more of the necessary criteria for revocation.<sup>27</sup> The criteria for revocation include: a Device Key has been copied and found in more than one device or product; a Key has been lost, stolen, intercepted, or otherwise misdirected, or made public or disclosed; a Network Key is present in more Terminal Modules than permitted by the Maximum Network Size; or SmartRight Applicants are required to revoke a Key by court order, or other competent government authority.<sup>28</sup> When a Content Participant provides the requisite proof to the SmartRight Association, revocation procedures *must* be initiated.<sup>29</sup> Thus, under the Content Participant Agreement, Content Participants have the direct right to initiate revocation procedures.

---

<sup>25</sup> See *SmartRight Content Participant Agreement* (“*SmartRight Content Participant Agreement*”) (attached hereto as Appendix B). This Agreement is modeled after the DTCP and HDCP Content Participant Agreements. SmartRight notes that both the DTCP and HDCP Content Participant Agreements each have been signed by two studios.

<sup>26</sup> *Id.* at § 3.2, 5.3.1

<sup>27</sup> *Id.* at § 5.3.1.

<sup>28</sup> *Id.* at § 5.3.2.

<sup>29</sup> *Id.* at § 5.3.1

Content Participants also have a significant role in the renewal process. Again, content participants are granted an express right to request renewal by filing an affidavit with the SmartRight Association reciting facts sufficient to meet the renewal criteria.<sup>30</sup> The criteria for renewal include: determination that unauthorized use or distribution of SmartRight content have reached a sufficient level to justify the cost of renewal; determination that it is feasible and desirable to upgrade the reliability and security of the SmartRight Technology; or a requirement to implement a change in outstanding SmartRight cards by court order, or other competent government authority.<sup>31</sup> Although the SmartRight Association reserves to itself the final determination on renewal because it is such a drastic, sweeping and costly measure, Content Participants are guaranteed meaningful participation in the process through their associate membership in the SmartRight Association.<sup>32</sup>

The SmartRight Content Participant Agreement, coupled with the third-party beneficiary rights afforded by the SmartRight Adopter Agreement, should provide the critical elements of protection to content providers that the MPAA Parties sought in their Opposition.

The SmartRight Applicants appreciate the MPAA Parties' view about the potential importance of the ATSC transport stream for the transmission of information related to revocation and renewal in the event of a compromise and would be pleased to work with content owners, other stakeholders, and the Commission to address this issue on a going-forward basis. The SmartRight Applicants anticipate the need to develop standardized methods for using the ATSC transport stream in the manner envisioned by MPAA and its members and establishment of appropriate FCC rules addressing the carriage and recognition of revocation and renewal

---

<sup>30</sup> *Id.*

<sup>31</sup> *Id.* at § 5.3.4.

<sup>32</sup> *Id.* at § 5.3.1.

information contained in the ATSC bit stream. The SmartRight system will comply with all applicable regulations that the Commission may adopt to address this issue.

**V. SMARTRIGHT PROVIDES FOR EFFECTIVE CHANGE MANAGEMENT PROCEDURES AND MEANINGFUL CONTENT OWNER PARTICIPATION**

The MPAA Parties oppose SmartRight's Certification on the grounds that it does not provide the terms and conditions under which content owners may play a meaningful role in the SmartRight change management process.<sup>33</sup> Again, this concern should be allayed by the new Content Participant Agreement.

The SmartRight Content Participant Agreement provides a detailed procedure which will enable content providers to object to any changes in the SmartRight system that they believe would have a material and adverse effect on the integrity or security of the SmartRight system, as well as to object to other changes to the SmartRight Adopter Agreement, including its Compliance Rules.<sup>34</sup> The SmartRight Authority is required to consider fully Content Participant objections to such changes and provide prompt written notice of a rejection of such objection, together with an explanation of the reasons therefore.<sup>35</sup> Should a majority of Major Content Participants<sup>36</sup> continue to object to the SmartRight Proposed Action, they have 30 days upon receipt of the rejection to initiate arbitration in accordance with the Content Participant Agreement.<sup>37</sup>

---

<sup>33</sup> See *MPAA Parties' Opposition* at 9-10.

<sup>34</sup> See *SmartRight Content Participant Agreement* at § 3.6.

<sup>35</sup> *Id.* at § 3.6.3.

<sup>36</sup> Major Content Participants are members of the MPAA, or like companies. See *SmartRight Content Participant Agreement* at § 1.35.

<sup>37</sup> *Id.* at § 3.6.4.



**VI. THE TERMS OF THE SMARTRIGHT ADOPTER AGREEMENT WILL APPLY TO ALL EQUIPMENT MANUFACTURERS, AND NO OBLIGATIONS ARE PLACED ON CONTENT OWNERS, BROADCASTERS, OR CONSUMERS BY VIRTUE OF DISTRIBUTING BROADCAST FLAG CONTENT**

The MPAA Parties object to the SmartRight certification on the grounds that it is concerned that the SmartRight License Agreement does not bind the SmartRight Applicants to the SmartRight Compliance and Robustness Rules as it does Adopters.<sup>38</sup> The MPAA Parties also seek assurance that the SmartRight License does not impose intellectual property licensing obligations on content owners, broadcasters, and consumers.<sup>39</sup>

SmartRight's Compliance and Robustness Rules apply equally to all equipment manufacturers, including those who also are SmartRight Applicants. A SmartRight Applicant, such as Thomson, seeking to manufacture and distribute products containing the SmartRight Technology system must sign an Adopter Agreement with the licensor, the SmartRight Authority, like any other entity.

SmartRight Applicants also understand the MPAA Parties' concern with respect to obligations associated with intellectual property. The SmartRight Authority will not assert its intellectual property in SmartRight against (a) content providers or broadcasters that are not SmartRight Content Participants or their affiliates as a result of their marking content with the Broadcast Flag in the United States, which engages the SmartRight content protection system under the Commission's Broadcast Flag rules, or (b) consumers as a result of their playing or recording of content in the United States that is marked by the Broadcast Flag, which triggers the SmartRight content protection system in accordance with the Commission's Broadcast Flag rules.

---

<sup>38</sup> See *MPAA Parties' Opposition* at 10-11.

<sup>39</sup> *Id.* at 11-12.

## **VII. CONCLUSION**

SmartRight Applicants believe that the clarifications and additional information contained in this Reply should adequately address questions and concerns raised by the MPAA Parties. Commission approval of the SmartRight system will bring needed competition, innovation and enhanced consumer flexibility to the digital content protection technology marketplace.

Respectfully submitted,

**THOMSON INC., ON BEHALF OF SMARTRIGHT APPLICANTS**



---

David H. Arland  
Vice President, U.S. Corporate Communications  
and Government Relations  
Thomson Inc.  
P.O. Box 1976, INH-430  
Indianapolis, IN 46206-1976  
(317) 587-4832

April 16, 2004

**APPENDIX A**  
**SMARTRIGHT ADOPTER AGREEMENT**  
**(APRIL 16, 2004)**



## ADOPTER AGREEMENT

### Evaluation License Convertible to Product License

This SmartRight® Adopter Agreement, (“Agreement”) is effective as of the latest date set out on the signature page hereof (the “Effective Date”) by and between the SmartRight Licensing Authority, LLC, (the “Authority”) and the Adopter named immediately below:

Name of Adopter:	
Description of Adopter’s Business	
Name of Contact Person:	
Contact Person’s Address, Phone Fax number E-mail Address:	
Location of Principal Office:	
Jurisdiction of Adopter’s Formation:	
Year of Formation:	
Number of Employees:	
Amount of Capital:	

## RECITALS

Whereas the Authority is the authorized Licensor of the SmartRight® system for protecting certain digital content from unauthorized use as described in the SmartRight Specification (the "Specification"); and

Whereas Adopter wishes to receive a license, subject to the terms and conditions set forth in this Agreement for the purpose of developing and evaluating and, at its option, implementing SmartRight, in accordance with the terms of this Agreement, including, but not limited to, the Compliance Rules annexed hereto.

Therefore, the Authority and Adopter agree as follows:

## TERMS OF AGREEMENT

### Article I.

#### DEFINITIONS

In addition to terms defined elsewhere in this Agreement, the following terms shall have the following meanings. All definitions herein shall apply equally to their singular and plural forms, all pronouns shall apply without regard to gender, and all references to Sections and Exhibits shall be deemed to be references to Sections of, and Exhibits to, this Agreement unless the context shall otherwise require.

1.1 **"Acquisition Device"** is defined in the Compliance Rules.

1.2 **"Activation"** means that the Adopter has executed the Activation Notice and has paid the fee referenced in Section 2.3, which is required to activate the Adopter's production license.

1.3 **"Adopter"** means the entity named at the beginning of this Agreement and includes its Affiliates.

1.4 **"Adopter Agreement"** means this Agreement and any other SmartRight Adopter Agreement entered into by the Authority and any other adopter of SmartRight.

1.5 **"Affiliate"** means with respect to any person or entity, any other person or entity directly or indirectly controlling or controlled by or under direct or indirect common control with such person or entity. "Control" means the possession of beneficial ownership of more than 50% of the stock or other similar interest entitled to vote for election of the Board of Directors or similar managing Authority.

1.6 **"Association"** means the SmartRight Association, Inc., a not for profit corporation established to administer the Renewal or Revocation of SmartRight Products on behalf of content providers, distributors and adopters in conformity with the Procedural Rules.

1.7 **"Certificate"** means a string of data bits attached to a Key for the purpose of identifying and validating the source of the Key.

1.8 **"Certified Key"** means a Key having an attached Certificate.

1.9 **"Combination Device"** is defined in the Compliance Rules.

1.10 **"Commercial Audiovisual Content"** is defined in the Compliance Rules.

1.11 **"Common Criteria"** means ISO/IEC 1540.

1.12 **"Compliance Rules"** means that document of the same name which is hereby incorporated into this Agreement by reference, as may be amended by the Authority from time to time. A Copy of the current Procedural Rules is annexed as Exhibit B to this Agreement.

1.13 **"Compliant"** means conforms in all respects to the Specification, the Compliance Rules and the Robustness Rules.

1.14 **"Conditional Access Content"** has the meaning set forth in the Compliance Rules.

1.15 **"Confidential Information"** means all information disclosed by either party to this Agreement that has been identified or designated to be confidential and proprietary, or that a reasonable person would judge to be confidential under the circumstances, including without limitation, any information concerning unpublished copyrighted works or mask works, unpublished pending patent applications, development materials, source code, unmarketed products or components, design documentation, system documentation specifications, and any information regarding such party's financial, business, and marketing matters. Except as provided in section 7.3.2, Confidential Information includes Highly Confidential Information. A party's status as an Adopter, or lack thereof, shall not be deemed Confidential Information.

1.16 **"Content Participant"** means a party who distributes or transmits, or cause or authorize the distribution or transmission of Conditional Access Content who has entered into an agreement with the Authority authorizing that party to protect its content through the use of the SmartRight System.

1.17 **"Converter Card"** means a SmartRight Smart Card intended for use with an Acquisition Device.

1.18 **"Device Key"** means a unique Certified Key which has been assigned to a particular Finished Licensed Product.

1.19 **"Essential Patent Claims"** means claims of a patent or patent application that would be necessarily and unavoidably infringed by the manufacture, use, sale, offer for sale or import or other disposition of a product or the practice of a method

required in order to comply with the SmartRight Specification in a particular country in the absence of a license or other authorization from the owner of such patent claims in such country. As used herein, "infringe" includes direct infringement, contributory infringement and/or inducement of infringement. Essential Patent Claims shall not include patent claims for a technology that has been developed by third parties independent of the SmartRight System but has been incorporated and referenced in the Specification for use in the SmartRight System.

1.20 **"Fellow Adopters"** means any entity other than the Adopter which has executed an Adopter Agreement and delivered it to the Authority or its designee.

1.21 **"Finished Licensed Product"** means an Acquisition Device, Presentation Device, Combination Device, Storage Only Device, Converter Card, or Terminal Card in a form that is intended to be distributed directly to end-users and which embodies any SmartRight Technology.

1.22 **"Generator"** means the Authority or an entity that has been retained by the Authority to generate Device Certificates and Device Keys for use by Adopters.

1.23 **"Highly Confidential Information"** means Confidential Information of the Authority that is marked or otherwise "Highly Confidential Information" or otherwise designated as such by the Authority. All Certified Keys are Highly Confidential Information.

1.24 **"Key"** means a string of information used by a cryptographic function either to encrypt, decrypt, sign, or check the signature of a message.

1.25 **"Licensed Marks"** means the trademark "SmartRight" in all jurisdictions in which it has been registered or adopted by the Authority and any other trademarks which the Authority by register or adopt for use in connection with Licensed Products.

1.26 **"Licensed Patents"** means all Essential Patent Claims of the patents and applications which the Authority has been authorized to license.

1.27 **"Licensed Product"** means a Finished License Product or a Licensed Component.

1.28 **"Licensed Component"** means a product, such as an integrated circuit, circuit board, or software module, that is designed to be incorporated into a Licensed Product and that embodies any SmartRight Technology.

1.29 **"Licensed Technology"** means the Licensed Patents, the Specification and all trade secrets, copyrights, mask rights and other exclusive rights which relate thereto and which the Authority owns or is authorized to license other than the Licensed Marks.

1.30 **“Local Enforcement Copy-Management Message” or “LECM”** means a data structure defined in the Specification which includes the Key necessary to decrypt SmartRight content and designates the content as “Copy Freely”, “View Only” or “Private Copy.”

1.31 **“Marked Content”** has meaning set forth in the Compliance Rules.

1.32 **“Maximum Network Size”** means the maximum number of terminal modules permitted to share the same Network Key on a PPN.

1.33 **“Network Key”** means a Key generated by a Terminal Module and used by all Terminal Modules on a PPN to decrypt an LECM created by a converter module associated with that PPN.

1.34 **“Party”** means the Authority or the Adopter.

1.35 **“Personal Private Network” or “PPN”** means a plurality of devices designed for the acquisition, storage, transmission, recording, reproduction and/or presentation of Commercial Audiovisual Content owned by the members of a single household and intended for use solely by the members of that household.

1.36 **“Presentation Device”** is defined in the Compliance Rules.

1.37 **“Procedural Rules”** means that document of the same name which is hereby incorporated into this Agreement by reference, as may be amended by the Authority from time to time. A Copy of the current Procedural Rules is annexed as Exhibit A to this Agreement.

1.38 **“Registered Owners”** means end-users who have purchased SmartRight Products and who have provided the Adopter with information sufficient to permit communications to be addressed to such person.

1.39 **“Renewal”** has the meaning ascribed in Section 4.1.

1.40 **“Renewal Criteria”** means those criteria for Renewal set forth in Section 4.3.

1.41 **“Revocation”** has the meaning ascribed in Section 4.1.

1.42 **“Revocation Criteria”** means those criteria for Revocation set forth in Section 4.2.

1.43 **“Rights”** means the Licensed Patents, the Licensed Technology and the Licensed Marks.

1.44 **“Robustness Rules”** means that document of the same name which is hereby incorporated into this Agreement by reference, as may be amended by



the Authority from time to time. A Copy of the current Procedural Rules is annexed as Exhibit C to this Agreement.

1.45 **“SmartRight Content”** means content that has been encrypted and packaged with a Local Enforcement Copy-Management Message ("LECM") in accordance with the SmartRight Specification. SmartRight Content includes Encrypted SmartRight Content and Decrypted SmartRight Content.

1.46 **“SmartRight Label”** means a holographic sticker or label issued by the Authority to be affixed to SmartRight Products for which a per unit license fee has been paid.

1.47 **“SmartRight Participants”** means the Authority, all Fellow Adopters and all Content Participants.

1.48 **“SmartRight Products”** means Compliant Finished Licensed Finished Products that have been qualified pursuant to sections 6.3 or 6.4. SmartRight Products may be Acquisition Devices, Presentation Devices or both.

1.49 **“Smart Card”** means either a Converter Card or a Terminal Card.

1.50 **“SmartRight Smart Cards”** means Smart Cards that are Qualified pursuant to Section 7.2. A Smart Right Smart Card may function as a Converter Card, a Terminal Card or both.

1.51 **“Specification”** means the specification entitled “SmartRight Specification” issued by the Authority, as may be amended from time to time pursuant to Section 3.3. **“Terminal Card”** means a SmartRight Smart Card intended for use in a Presentation Device.

1.52 **“Terminal Module”** means a Terminal Card or an integrated module in a Presentation Device which performs the functions of a Terminal Card.

## Article II.

### FEEES

2.1 **Current Fees and Modifications.** The Fees currently chargeable by the Authority to Adopters are set out in Procedural Rules. The Authority may, upon at least thirty (30) days notice to Adopter, modify the Annual Administration Fee and Certificate Fees payable for the period beginning on the next Annual Payment Date, provided that any increase in such fees shall not exceed an amount commensurate with any increase in the Authority's costs (including but not limited to the cost of inflation). Without limiting the foregoing, where costs per Certificate or per Adopter decrease, the Authority shall use commercially reasonable efforts to reduce the Per Certificate Fee or Annual Administration Fee, respectively.

2.2 **Annual Administration Fee, Evaluation Rights.** Within thirty (30) days of the Effective Date, Adopter shall pay the Authority a nonrefundable sum in

the amount of the Annual Administration Fee for Evaluation Rights set out in the Procedural Rules (the Adopter shall not be entitled to any refund thereof for any reason). Upon each anniversary of the Effective Date (the “Annual Payment Date”), or such other date as specified in the Procedural Rules, Adopter shall pay the Authority the Annual Administration Fee for the following year,

**2.3 Annual Administration Fee, Production Rights.** At any time following the Effective Date, Adopter may Activate the Production License granted under Section 5.2 by payment of an Annual Administrative Fee for Production Rights in the amount set forth in the Procedural Rules and submitting of an Activation Notice in the form promulgated by the Authority. To the extent the Adopter has previously paid a fee for Evaluation Rights for the then current year, a pro-rated portion of such fee for the period remaining until the next Annual Payment Date shall be credited against its Annual Administrative Fee for Production Rights. Following Activation, the Adopter’s Annual Payment Date shall be the anniversary date of its initial Activation, or such other date as specified in the Procedural Rules.

**2.4 Certified Key Fees.** Certified Device Keys are necessary to manufacture some Licensed Products. Certified Device Keys are generated by the Generator under the direction of the Authority. Following Activation, Certified Device Keys shall be made available according to the fee schedule set out in the Procedural Rules, as updated from time to time in accordance with the terms of this Agreement. Prior to Activation, Facsimile Certified Device Keys shall be issued to Adopter for development purposes only. Such facsimile Certified Devices Keys will not inter-operate with commercial devices and Devices which incorporate facsimile Certified Keys will not be deemed Licensed Products within the meaning of this Agreement.

**2.5 Per Unit Royalty.** In addition to the Annual Administrative Fee, set forth in Section 2.3, above, Adopter will pay a royalty fee of \$2.00 per unit in advance for each SmartRight Product sold by Adopter. Upon receipt of such payment, the Authority will issue a SmartRight Label to be affixed by the Adopter to each product prior to sale to authenticate that a per unit royalty has been paid with respect to that product.

**2.6 Reference Implementations.** The Authority will make reference implementation components available to Adopter for inclusion in Acquisition and Presentation Devices in return for fees as specified in the Procedural Rules.

**2.7 Manner of Payment.** All fees shall be paid to the Authority or to its order in United States dollars by wire transfer or such other means as the Authority may reasonably specify. Adopter shall be responsible for payments of any taxes or charges imposed by the Authority by reason of such fees. If Adopter is required by law to make any withholding from fees due to the Authority, it may make such withholding but shall provide the Authority, at the time of payment, with evidence of such withholding adequate to permit the Authority or its assignee to claim the relevant credit for the amounts withheld.

Article III.  
**SPECIFICATION AND COMPLIANCE RULES**

3.1 **Delivery.** Upon Adopter's execution hereof and the Authority's receipt of the Administration and Disclosure Fee, the Authority shall cause to be distributed to Adopter the relevant portions of the Specification that Adopter has not previously received.

3.2 **Distribution.** Adopter agrees to provide copies of the Specification and Compliance Rules to those persons having supervisory responsibility for the design and manufacture of Licensed Products and Licensed Components for and on behalf of Adopter, in such manner and at such times as to promote Adopter's compliance with all applicable terms thereof.

3.3 **Changes.**

3.3.1 The Specification and the Compliance Rules may be amended from time to time by the Authority only in accordance with this Section 3.3. Adopter shall be required to comply with all amendments to the Compliance Rules and the Specification within eighteen months after the later of (a) delivery of a notice to the Adopter and interested Content Participants of such change in accordance with Section 11.7 or (b) the issuance of an award in an arbitration pursuant to Section 3.3.4(b). Changes in the Procedural Rules, with the exception of the Annual Administration Fees and Certified Key Fees, shall be effective on no less than thirty days' notice. Changes to the Annual Administration Fees or Certified Key Fees shall be permitted only as set out in Section 2.1. Changes in Per Unit Royalties shall be effective on no less than one year's notice.

3.3.2 The Authority shall not make any material changes to the Specification (including any changes that would expand the Specification to require new technical features not included in the version of the Specification in effect as of the Effective Date that can not be implemented by the issuance of new Smart Cards or would otherwise create compatibility problems with Licensed Products manufactured prior to such changes); provided, however, that the Authority may make such limited changes, if any, in the Specification as would permit SmartRight to be used with transports other than those permitted in version of the Specification as may be in effect as of the Effective Date. Without limiting the foregoing, the Authority reserves the right to correct any errors or omissions in the Specification or to make changes that would clarify, but not materially amend, alter or expand the Specification, from time to time.

3.3.3 Except as the Authority may conclude is necessary to comply with regulations of the FCC or other applicable governmental authority, the Authority shall not make any revisions to the Compliance Rules that would materially increase the cost or complexity of implementations of SmartRight Licensed Products.

3.3.4 In the event Adopter, together with one unaffiliated Fellow Adopters notifies the Authority within sixty days after receiving notice of the change,

that it has a bona fide objection to the change on the grounds specified in Sections 3.3.2 or 3.3.3, then the following procedures shall apply:

(a) The Authority, interested Content Participants, and the Adopters shall attempt in good faith to resolve the objections to the proposed change during the sixty day period following the delivery of the notice of the objections.

(b) At any time during such sixty day period, any Adopters who have filed timely objections may request arbitration to resolve the dispute by sending to the Authority a notice of intention to arbitrate in accordance with the commercial arbitration rules of the American Arbitration Association (the "Rules"). The parties shall thereafter proceed to arbitrate the dispute before a single arbitrator in the City of New York under the expedited procedures set forth in the Rules, except that the arbitrator shall render his or her award no later than 180 days following the commencement of the arbitration.

#### Article IV.

### REVOCATION AND RENEWAL

4.1 **Generally.** The Specification includes means by which Keys may be invalidated (generally, "Revocation" or "Revoke"). SmartRight Smart Cards and all attributes of SmartRight Products capable of being modified by a Smart Card may also be replaced or modified through the distribution of new SmartRight Smart Cards (generally, "Renewal" or "Renew"). By entering into this agreement, the Adopter hereby consents to grant to the SmartRight Association, Inc. (the "Association"), the right to determine whether any or all Certified Keys issued to the Adopter may be Revoked or SmartRight Products Renewed in accordance with this Article IV and the procedures set forth in the Procedural Rules.

4.2 **Revocation.** The Association may Revoke a Key when it is required to do so pursuant to Section 4.2.4 or it has otherwise been determined, pursuant to the procedures set forth in the Procedural Rules, that one or more of the Revocation Criteria have been satisfied. The "Revocation Criteria" mean the following:

4.2.1 A Device Key has been copied such that the same Key is found in more than one device or product;

4.2.2 A Key has been lost, stolen, intercepted or otherwise misdirected, or made public or disclosed; or

4.2.3 A Network Key is present in more Terminal Modules than permitted by the Maximum Network Size.

4.2.4 The Association is required to revoke a Key by court order, or other competent government Authority.

4.3 **Renewal.** The Association may Renew any or all outstanding SmartRight Smart Cards when it is required to do so pursuant to Section 4.3.3 or it has otherwise been determined, pursuant to the procedures set forth in the Procedural Rules, that one or more of the Renewal Criteria have been satisfied. The "Renewal Criteria" mean the criteria set forth in Sections 4.3.1, 4.3.2 or 4.3.3:

4.3.1 The Association determines that unauthorized use or distribution of SmartRight content have reached a sufficient level to justify the cost of Renewal.

4.3.2 The Association determines that it is feasible and desirable to upgrade the reliability and security of the SmartRight Technology.

4.3.3 The Association is required to implement a change in outstanding SmartRight Smart Cards by court order, or other competent government Authority.

4.4 **Procedure.** The procedures set out in the Procedural Rules shall govern Revocation and Renewal. Such procedures provide for notice and review of the Association decisions and/or actions regarding Revocation where requested.

## Article V. LICENSES

5.1 **Evaluation License.** Upon execution of this Agreement, and so long as it remains in effect, Authority grants to Adopter (including its Affiliates) a non-exclusive, nontransferable, nonsublicenseable, worldwide license to use the Licensed Technology solely for the purpose of evaluating and developing Licensed Products.

5.2 **Production License.** Upon Activation, the Authority grants to Adopter and its affiliates a nonexclusive, nontransferable, nonsublicenseable, worldwide license under the Licensed Technology to make, have made, use, import, offer to sell and sell Licensed Products; provided that such license shall not extend to features of a product that are not required to comply with the Specification, provided, however, that the license to sell granted hereunder shall not apply to the sale of Licensed Finished Products unless (a) a SmartRight Label has been affixed to the product and (b) the Product has been qualified as a SmartRight Product pursuant to Section 6.3 or 6.4.

5.3 **Trademark License.** Upon Activation, and subject to the trademark usage guidelines adopted by the Authority, the Authority grants to Adopter (including its Affiliates) a nonexclusive, nontransferable, nonsublicenseable, worldwide license to use the Licensed Marks solely in connection with the sale, distribution and marketing of SmartRight Products that have been qualified pursuant to section 6.3 or 6.4.

5.4 **Copyright License.** The Authority grants to Adopter and its Affiliates a nonexclusive, nontransferable, worldwide license to reproduce, modify and pre-

pare derivative works based upon any copyrighted works or mask works included in the Licensed Technology solely to the extent reasonably necessary to comply with the Specification and the requirements of this Agreement; provided, however, that the license granted hereunder shall not apply to Highly Confidential Information except as expressly authorized pursuant to Section 7.3.1(c)

**5.5 Reciprocal Licensing Agreement.** In the event Adopter, now or in the future, owns or controls any Essential Patent Claims, Adopter shall, either (a) not assert such claims against any SmartRight Participant making, having made, using, importing, offering to sell or selling Licensed Products, or for engaging in any activities for which any of those persons have been granted a license by the Authority, or (b) offer to license all SmartRight Participants under any Essential Patent Claims owned or controlled by Adopter or its Affiliates on terms that are fair, reasonable and non-discriminatory, the right to make, have made, use, import, offering to sell and sell Licensed Products.

**5.6 Proper Use.** The licenses granted herein are subject to and conditioned on the requirement that Adopter shall not produce or sell any devices or software where such devices or software are designed to circumvent the Compliance Rules, the Robustness Rules or the effectiveness of the Specification.

**5.7 Restrictions on Authority.** The Authority shall not engage in the manufacture, distribution or sale of SmartRight Products, nor shall it license others to so except pursuant to an Adopter Agreement substantially in the form of this Agreement.

## Article VI.

### DISTRIBUTION AND QUALIFICATION OF PRODUCTS

**6.1 Licensed Products Qualified.** Qualified SmartRight Products may be disposed of in any commercially reasonable manner.

**6.2 Licensed Components.** Licensed Components may only be furnished to Fellow Adopters and persons or entities providing products or services to Adopter pursuant to the right under Section 5.2 to “have made” Licensed Products (a “Have Made Party”). Licensed Components (Schedule 2) may only be furnished to Fellow Adopters and Have Made Parties. Adopter shall contractually bind any Have Made Party to sell, distribute or otherwise dispose of Licensed Components furnished by or made for Adopter only to Adopter.

**6.3 Qualification of SmartRight Products, Self Test.** The Authority will provide each Adopter with self-qualification test-suites. To be qualified as a SmartRight Licensed Finished Product and be allowed to bear the License Mark, each model of a proposed SmartRight Licensed Finished Product must be fully Compliant and must successfully pass the tests included in the self-qualification test-suite. Terminal Smart Cards must be compliant with the Common Criteria and successfully pass the ISO/IEC 15408 certification to be qualified as SmartRight Licensed Smart Card. Upon successfully completing the self-qualification test-suite, the Adopter shall notify the Authority of each

self-qualified product model and provide the Authority with a completed qualification checklist, including test results, in a form to be provided by the Authority and a copy of the service manual therefor.

**6.4 Qualification of SmartRight Products by the Authority.** The Authority shall provide a Qualification Service which will perform the tests necessary to qualify SmartRight Licensed Finished Products and SmartRight Cards upon request of the Adopter for a reasonable and non-discriminatory fee. If the Adopter wishes to use this service, a sample of the Device and a copy of its service manual must be submitted to the Authority or a contractor designated by the Authority for such purpose and such model must be approved as Compliant by the Authority or its designee. SmartRight Smart Cards must be compliant with ISO/IEC 15408, and successfully pass the ISO/IEC 15408 certification to be qualified as SmartRight Licensed Smart Card.

**6.5 No Sales of Non-qualified Products.** Sale of non-Qualified Finished License Products, or any other devices bearing the Licensed Marks, will constitute a material breach of this Agreement subject to the remedies set forth in Article X in addition to any other remedies as may be available to any party. If any Finished Licensed Products sold by Adopter are determined to be non-Compliant, the Authority may require that Adopter withdraw such products from the market.

**6.6 Compliance with Laws, Export.** Adopter will comply with all applicable rules and regulations of the United States, Japan, Member States of the European Union, and other countries and jurisdictions, including those relating to the export or re-export of commodities, software and technical data insofar as they relate to the activities under this Agreement. Adopter is aware that commodities, software and technical data provided under this Agreement may be and/or are subject to restrictions under the export control laws and regulations of the United States, Japan, Member States of the European Union and other countries and jurisdictions, as applicable, including but not limited to the U.S. Export Administration Act and the U.S. Export Administration Regulations, any relevant and applicable European Union rules and procedures (including rules and procedures of the Member States of the European Union), and the Japanese Foreign Exchange and Foreign Trade Law, and shall obtain any approval required under such laws and regulations whenever it is necessary for such export or re-export.

## Article VII.

### CONFIDENTIALITY

**7.1 Permitted Uses.** A Party who receives Confidential information (the "**Receiving Party**") shall use any Confidential Information (and tangible embodiments of any of the foregoing) disclosed to it by the other Party (the "**Disclosing Party**") solely for purposes of exercising its rights and performing its obligations under this Agreement.

**7.2 No Circumvention.** During the Confidentiality Period set forth in Section 7.9 below, Adopter shall not itself nor assist others in producing any devices or

software designed to circumvent the Compliance Rules or the effectiveness of the Specification

### 7.3 **Preservation of Confidentiality.**

7.3.1 **Highly Confidential Information.** Adopter shall maintain the confidentiality of Highly Confidential Information in the following manner:

(a) Adopter shall employ procedures for safeguarding Highly Confidential Information at least as rigorous as Adopter would employ for its own most highly confidential information, such procedures to include, at a minimum: (1) maintaining on Adopter's premises a secure location in which any and all Highly Confidential Information shall be stored; (2) such secure location shall be accessible only by authorized employees; (3) employees shall sign in and out each time such employees visit such secure location; and (4) when Highly Confidential Information is not in use, such information shall be stored in a locked safe at such secure location. The foregoing procedures shall not apply to Certified Keys embedded in a SmartRight Smart Card.

(b) Adopter may disclose Highly Confidential Information only to (i) the minimum possible number of regular employees of Adopter: (1) who have an absolute need to know such Highly Confidential Information in order to enable Adopter to implement SmartRight Technology in compliance with the Specification; and, (2) who are bound in writing by obligations of confidentiality sufficient to protect the Highly Confidential Information in accordance with the terms of this Agreement; and, (b) Have Made Parties who have entered into an agreement with the Authority consistent with the provisions hereof that authorizes such third party to receive such Highly Confidential Information. Distribution of a SmartRight Smart Card or Presentation Device in which a Certified Key has been embedded shall not constitute disclosure for purposes of this section.

(c) Adopter shall not make any copies of any Highly Confidential Information, except that a single copy of a Certified Key may be made for the purpose of embedding a Certified Key into a single Terminal Module, following which the original copy shall be destroyed. If reasonably required for purposes of this agreement, Adopter may request additional copies of such information and the Authority may in its sole discretion fulfill any such request.

7.3.2 **Other Confidential Information.** A Receiving Party may disclose Confidential Information of the Disclosing Party, other than Highly Confidential Information, only to employees and individuals retained as independent contractors subject to confidentiality obligations equivalent to those applicable to its own employees and contractors who have a reasonable need-to-know and are bound in writing by obligations of confidentiality sufficient to protect the Confidential Information in accordance with the terms of this Agreement. Each Receiving Party shall use the same degree of care, but no less than a reasonable degree of care, to avoid unauthorized disclosure or use of Confidential Information as such party employs with respect to its comparably important confidential information.



7.4 **Cooperation and Assistance.** Each Party receiving Confidential Information shall make all reasonable efforts to assist the Disclosing Party in relation to any claim, action, suit, proceeding, or litigation with respect to any improper or unauthorized use or disclosure of Confidential Information by any present or former employees of the Receiving Party or any third parties who have obtained Confidential Information from it.

7.5 **Contact Person.** Adopter shall designate a single employee and an alternate employee who shall receive all Confidential Information and Highly Confidential Information (the "Adopter Contact") disclosed by the Authority.

7.6 **Notification of Unauthorized Use or Disclosure.** Each Party shall notify the other Party in writing immediately upon discovery of any unauthorized use or disclosure of Proprietary Information, and will cooperate with the Authority in every reasonable way to regain possession of Proprietary Information and prevent its further unauthorized use or disclosure.

7.7 **Disclosure Required by Law.** If a Receiving Party is required by law, regulation or order of a court or other Authority of competent jurisdiction to disclose Confidential Information, such Receiving Party shall promptly notify the Disclosing Party and shall make reasonable efforts to challenge the discloser or secure an appropriate protective order restricting the scope of use and disclosure of the Confidential Information.

7.8 **Confidentiality Exceptions.** The restrictions contained in this Article VII shall not apply to information that the Receiving Party can demonstrate by documentary evidence: (i) has been generally known to the public through no breach of the Receiving Party's obligations for more than 120 days and the Disclosing Party has failed to institute reasonable measures to remove it from public availability or enjoin further public disclosure, (ii) was in the possession of the Receiving Party prior to its Disclosure by the Disclosing Party, (iii) was developed by the Receiving Party's employees (whether independently or jointly with others) without having access (whether directly or through any intermediaries) to such Confidential Information and without any breach of its obligations hereunder, or (iv) is or has been disclosed to the Receiving Party by a third party that had developed (whether independently or jointly with others) such information without any access (whether directly or through any intermediaries) to any Confidential Information and without any breach of any such third party's obligations to the Disclosing Party. Notwithstanding the foregoing, any Certified Keys provided to the Adopter shall not lose their status as Highly Confidential Information.

7.9 **Confidentiality Period.** The confidentiality obligations set forth herein shall continue until five years after the last commercial use of SmartRight Technology by the Authority or any Fellow Adopter.

Article VIII.  
**TERM/TERMINATION**

8.1 **Termination.** This Agreement shall be effective upon the Effective Date and shall continue until terminated in accordance with any of the following events:

8.1.1 **Termination by Adopter.** Adopter shall have the right to terminate this Agreement at any time upon 90 days' prior written notice to the Authority.

8.1.2 **Termination for Breach.** In the event that either party (i) materially breaches any of its obligations hereunder, which breach is not cured within 30 days after written notice is given to the breaching party specifying the breach; or (ii) repeatedly breaches any of its obligations hereunder and fails to cure and cease committing such repeated breaches within 30 days after being given written notice specifying the breaches, then the party not in breach may, by giving written notice thereof to the breaching party, terminate this Agreement, upon the expiration of the 30 day period beginning on the date of such notice of termination.

8.2 **Effect of Termination.** Upon termination or expiration of this Agreement, Adopter shall immediately cease use of Certified Keys. Within 30 days after termination or expiration of this Agreement, (i) Adopter shall return such Certified Keys (ii) each party shall return all other Confidential Information to the Authority; or (ii) destroy all Confidential Information in its possession, retaining no copies thereof, and certify such destruction in writing to the Authority. Within 30 days after termination or expiration of this Agreement, Adopter shall discontinue all manufacture, sale, or distribution of SmartRight Licensed Products.

8.3 **Survival.** Following termination of this Agreement for any reason, the following provisions shall survive: Sections 5.5, 5.6 and 6.5 and Articles VII, VIII, IX, X and XI.

Article IX.  
**DISCLAIMER AND LIMITATION OF LIABILITY**

9.1 **Generally.** The following terms limit the ability of the Adopter to recover any damages from the Authority in excess of fees actually paid to the Authority by Adopter during a one year period. These provisions are an essential part of the bargain, without which the Authority would not be willing to enter into this Agreement.

9.2 **Warranty Disclaimer.** ALL INFORMATION, MATERIALS, KEYS, AND CERTIFICATES ARE PROVIDED "AS IS." THE AUTHORITY AND THE MEMBERS AND CERTIFICATION AUTHORITY MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND EXPRESSLY DISCLAIM IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION THAT MIGHT ARISE FROM ANY ACTIVITIES OR INFORMATION DISCLOSURES RELATING TO THIS AGREEMENT. THE AUTHORITY FURTHER DISCLAIMS ANY WARRANTY THAT ANY IMPLEMENTATION OF THE SPECIFICATION, IN WHOLE OR IN PART, WILL BE FREE FROM INFRINGEMENT OF ANY THIRD PARTY INTELLECTUAL PROPERTY OR PROPRIETARY RIGHTS.

9.3 **Limitation of Liability.** THE AUTHORITY NOR ITS MEMBERS NOR ANY DIRECTOR, OFFICER, AGENT, MEMBERS, REPRESENTATIVES, EQUIVALENT CORPORATE OFFICIALS, OR EMPLOYEE OF ANY OF THEM ACTING IN THEIR CAPACITIES AS SUCH (COLLECTIVELY, THE "AFFECTED PARTIES") SHALL BE LIABLE TO ADOPTER FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR PUNITIVE DAMAGES ARISING OUT OF ANY CAUSE OF ACTION RELATING TO THIS AGREEMENT, OR BASED ON MAKING, USING, SELLING OR IMPORTING ANY PRODUCTS OF ADOPTER THAT IMPLEMENT PROPRIETARY INFORMATION OR SMARTRIGHT TECHNOLOGY, WHETHER UNDER THEORY OF CONTRACT, TORT, INDEMNITY, PRODUCT LIABILITY OR OTHERWISE. TO THE EXTENT THAT ANY COURT OF COMPETENT JURISDICTION RENDERS JUDGMENT AGAINST THE AUTHORITY NOTWITHSTANDING THE ABOVE LIMITATION, THE AFFECTED PARTIES' AGGREGATE LIABILITY TO ADOPTER IN CONNECTION WITH THIS AGREEMENT SHALL IN NO EVENT EXCEED THE AMOUNTS OF MONEY RECEIVED BY THE AUTHORITY FROM ADOPTER UNDER THIS AGREEMENT IN ANY ONE YEAR PERIOD.

## Article X. **REMEDIES**

10.1 **Indemnification for Wrongful Acts of Adopter.** Adopter shall indemnify and hold the Authority, the Members, the Generator, and their officers, members, representatives, agents, directors, equivalent corporate officials, and employees, harmless from and defend against any claims, actions, suits, proceedings or litigation, and any losses, deficiencies, damages, liabilities, costs and expenses including without limitation, reasonable attorneys' fees and all related costs and expenses, to be paid or otherwise incurred in connection with the defense of any claim, action, suit, proceeding or litigation, that arises from any material breach of any covenant, agreement, representation or warranty herein or claimed wrongdoing by the Adopter.

**10.2 Equitable Relief.** The Authority and Adopter agree and acknowledge that, due to the unique nature of certain provisions hereof, the lasting effect of and harm from a breach of such provisions, including the potential for widespread unauthorized distribution of copyrighted content intended to be protected using the Specification, if a Party breaches its obligations hereunder, money damages alone may not adequately compensate an injured party, and that injury to such party may be irreparable, and that specific performance or injunctive relief is an appropriate remedy to prevent further or threatened breaches hereof.

**10.3 Liquidated Damages Measure and Limitation.** The parties agree that it would be difficult to ascertain the amount of damages in the event of certain breaches of its obligations by Adopter and that damages therefor shall be liquidated as follows:

10.3.1 In the event of a material breach by Adopter of the provisions of Article VII, that results in the unauthorized use or disclosure of Confidential Information by a third party, Adopter shall be liable for \$1 million dollars;

10.3.2 In the event of the distribution of devices or software that fail to adequately protect Keys and Certificates as required by the applicable Compliance Rules, and result in the unauthorized use or disclosure of such Keys and/or Certificates, Adopter shall be liable in an amount equal to its profits on such devices or software, but in no event less than \$1 million dollars nor more than \$8 million;

10.3.3 Notwithstanding the foregoing, Adopter shall not be liable for liquidated damages if (a) Adopter maintains an internal program to assure compliance herewith (including a program to assure maintenance of inventory, samples, and confidentiality of information for purposes in addition to compliance with this Agreement), (b) the breach was inadvertent or otherwise unintentional, (c) the breach did not have a material adverse effect on the integrity or security of SmartRight Technology or the function of SmartRight Technology to protect Commercial Audiovisual Content and (d) if the Adopter was aware of the breach, it brought the breach to the Authority's attention in a timely manner;

10.3.4 The parties agree and expressly acknowledge that amounts which may be payable by Adopter as contemplated in this Section 10.3 are a reasonable estimate of the damages that the Authority may sustain upon the occurrence of the events giving rise to such payments and that such amounts are reasonable and appropriate, since it would be impracticable or extremely difficult to determine the exact amount of the Authority's damages resulting from the specific acts giving rise to such payments. Said amounts are not to be construed in any sense to be a penalty and shall be considered adequate compensation to the Authority with respect to the acts giving rise to such payments.

**10.4 Third Party Rights of Content Providers and Others.** Compliance of Adopter and other licensees with the terms hereof is essential to maintain the

value, integrity, security and performance of SmartRight Technology. As part of the consideration granted herein, upon Activation, Adopter agrees that (i) third parties who distribute or transmit, or cause or authorize the distribution or transmission of Marked Content, (ii) Content Participants (iii) Fellow Adopters who are not in material breach of any term or condition of their Adopter Agreement are beneficiaries of this Agreement and may bring a claim or action to enforce this Agreement against Adopter (a "Third Party Beneficiary Claim") in accordance with the procedures set out in the Procedural Rules. Such claims shall be limited to seeking injunctive relief against the manufacture, distribution, commercial use and sale of Adopter's products that are in material breach of the Compliance Rules, and against disclosure of Highly Confidential Information in breach of this Agreement that affects the integrity or security of SmartRight Technology, except that where such Adopter has willfully breached, or engaged in a pattern or practice of breaching, such obligations, in which case attorneys' fees and costs shall be awarded to each third party that is a prevailing party.

## Article XI. MISCELLANEOUS

11.1 **Ownership.** All SmartRight Technology provided by the Authority to Adopter shall remain the property of the Authority or its licensors. Except as expressly provided herein, this Agreement does not give Adopter any other license rights to the SmartRight Technology.

11.2 **Entire Agreement.** This Agreement, the exhibits hereto and the Specification constitute the entire Agreement between the parties hereto with respect to the subject matter hereof and supersede all prior oral, written or other agreements. Except as otherwise provided herein, this Agreement may not be modified except by written agreement dated subsequent to the date of this Agreement and signed by both parties.

11.3 **Controlled Entities.** Adopter represents and warrants that its Affiliates will comply with the terms of this Agreement and that it shall be responsible for the acts of its Affiliates to the same extent as if it performed those acts itself.

11.4 **Assignment.** The licenses granted hereunder are personal to Adopter, and Adopter's rights under this Agreement shall not be assigned or otherwise transferred except (a) with the written approval of the Authority (which shall not be unreasonably withheld) or (b) to a legal entity controlling, controlled by or under common control with Adopter or to the purchaser of all or substantially all of the outstanding capital stock or assets and obligations of Adopter or to the surviving entity in a merger, reorganization, or other business combination and where notice of such assignment has been provided in advance to the Authority and where the surviving or acquiring company agrees in writing to be bound by this Agreement. Subject to the limitations set forth in

this Agreement, this Agreement will inure to the benefit of and be binding upon the parties, their successors and permitted assigns. The Authority may assign or transfer this Agreement to a party that agrees to assume the Authority's obligations hereunder, and will provide Adopter with written notice thereof.

**11.5 Presumptions.** In construing the terms of this Agreement, no presumption shall operate in either party's favor as a result of its counsel's role in drafting the terms or provisions hereof.

**11.6 Governing Law; Jurisdiction.** THIS AGREEMENT, AND ALL THIRD-PARTY-BENEFICIARY CLAIMS BROUGHT PURSUANT HERETO, SHALL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF NEW YORK APPLICABLE TO AGREEMENTS MADE AND TO BE PERFORMED ENTIRELY IN SUCH STATE AND WITH THE LAWS OF THE UNITED STATES AS WOULD BE CONSTRUED BY A COURT SITTING IN THE SOUTHERN DISTRICT OF NEW YORK.

**11.6.1** ANY LITIGATION BETWEEN THE PARTIES HERETO AND ANY THIRD-PARTY-BENEFICIARY CLAIM ARISING OUT OF OR RELATING TO THIS AGREEMENT SHALL BE SUBJECT (i) THE EXCLUSIVE JURISDICTION AND VENUE IN THE FEDERAL AND STATE COURTS LOCATED IN THE COUNTY OF NEW YORK, NEW YORK, (EXCEPT THAT CLAIMS BROUGHT PURSUANT TO SECTION 10.4 MAY BE BROUGHT IN A COURT SITTING IN LOS ANGELES COUNTY, CALIFORNIA); AND (ii) THE SERVICE OF PROCESS OF SAID COURTS BY PERSONAL DELIVERY OR BY MAILING OF PROCESS BY REGISTERED OR CERTIFIED MAIL, POSTAGE PREPAID, AT THE ADDRESSES SPECIFIED IN THIS AGREEMENT.

**11.6.2** ADOPTER SHALL APPOINT AN AGENT IN THE STATE OF NEW YORK FOR ACCEPTANCE OF SERVICE OF PROCESS PROVIDED FOR UNDER THIS AGREEMENT AND SHALL NOTIFY THE AUTHORITY OF THE IDENTITY AND ADDRESS OF SUCH AGENT WITHIN THIRTY (30) DAYS AFTER THE EFFECTIVE DATE.

**11.6.3** ADOPTER WAIVES ANY OBJECTION TO THE JURISDICTION, PROCESS, AND VENUE OF ANY SUCH COURT, AND TO THE EFFECTIVENESS, EXECUTION, AND ENFORCEMENT OF ANY ORDER OR JUDGMENT (INCLUDING, BUT NOT LIMITED TO, A DEFAULT JUDGMENT) OF SUCH COURT PERTAINING TO THIS AGREEMENT, IN ANY OTHER JURISDICTION TO THE MAXIMUM EXTENT PERMITTED BY THE LAW OF THE PLACE WHERE ENFORCEMENT OR EXECUTION OF ANY SUCH ORDER OR JUDGMENT MAY BE SOUGHT AND BY THE LAW OF ANY PLACE WHOSE LAW MIGHT BE CLAIMED TO BE APPLICABLE REGARDING THE EFFECTIVENESS, ENFORCEMENT, OR EXECUTION OF SUCH ORDER OR JUDGMENT, INCLUD-

ING PLACES OUTSIDE OF THE STATE OF NEW YORK AND OF THE UNITED STATES. ADOPTER AND THE AUTHORITY WAIVE ANY RIGHTS THEY MAY HAVE TO A JURY TRIAL.

11.7 **Notice.** All notices to be provided pursuant to this Agreement shall be given in writing and shall be effective when either served by personal delivery or upon receipt via certified mail, return receipt requested, postage prepaid, overnight courier service or sent by facsimile transmission with hard copy confirmation sent by certified mail, in each case to the party at the addresses set out herein.

11.8 **Severability; Waiver.** Should any part of this Agreement judicially be declared to be invalid, unenforceable, or void by any court of competent jurisdiction, the parties agree that the part or parts of this Agreement so held to be invalid, unenforceable, or void shall be reformed by such court without further action by the parties hereto but only to the extent necessary to make such part or parts valid and enforceable. A waiver by either of the parties hereto of any of the covenants to be performed by the other party or any breach thereof shall not be effective unless made in writing and signed by the waiving party and shall not be construed to be a waiver of any succeeding breach thereof or of any covenant herein contained.

11.9 **Most Favored Status.** The Authority will make available to Adopter the terms of its current standard Adopter Agreement, and any clarifications or interpretations of the provisions of its Adopter Agreement by posting them on the Authority website or otherwise. The Authority also commits that the benefit of any modification, clarifications or interpretations of language in the standard Adopter Agreement will be extended to Adopter in accordance with this section. Where the Authority agrees to make a change to a particular Fellow Adopter's standard Adopter Agreement, such change shall be reflected in the next regular revision of the standard Adopter Agreement. Upon the promulgation of such revision, Adopter will be given the option to substitute such revised Adopter Agreement for this Agreement. Prior to such time as it makes a revised standard Adopter Agreement available to all Fellow Adopters that have executed a standard Adopter Agreement, where the Authority has agreed to include language in a particular Fellow Adopter's standard Adopter Agreement that is more favorable than that in the then-current version of the standard Adopter Agreement, the Authority will not enforce the language in Adopter's Adopter Agreement to the extent that such language is less favorable than that found in such Fellow Adopter's Adopter Agreement. For purposes of this Section 11.9, "standard Adopter Agreement" refers to an Adopter Agreement under which a Fellow Adopter receives a license with respect to activities that are equivalent to all activities licensed hereunder, but does not include, by way of example and not limitation, any Adopter Agreement in which a Fellow Adopter is not licensed to manufacture or to sell Licensed Products.

**IN WITNESS WHEREOF,** the parties have executed this Agreement as of the date first above written.

THE AUTHORITY:

ADOPTER:

By: \_\_\_\_\_

By: \_\_\_\_\_

Name:

Name:

Title:

Title:

Date:

Date:

Addresses for notices:

THE AUTHORITY:

ADOPTER:



**SMARTRIGHT ADOPTER AGREEMENT****EXHIBIT A****PROCEDURAL RULES EFFECTIVE JANUARY 1, 2004**

Unless otherwise expressly stated in this Procedural Rules, all section references in this Procedural Rules are references to sections of this Procedural Rules.

**1. FEE SCHEDULE****1.1 Annual, Certified Key and Per Unit Fees:**

<b>Category of License</b>	<b>Annual Administration Fee</b>	<b>Certified Key Fee</b>	<b>Per Unit License Fee (SmartRight Label)</b>
Evaluation Rights	\$10,000	\$0.10	N/A
Production Rights	\$30,000	\$0.10	\$2.00

Shipping and Handling: \$200 per order.

All Certified Keys are Highly Confidential Information and shall be subject to the requirements of Section 7.3.1 of the Adopter Agreement.

**1.2 Procedure For Ordering Keys and SmartRight Labels.** Adopter will be supplied with a form and associated tools for ordering Keys and SmartRight Labels. The number of Keys and SmartRight Labels that may be ordered will be constrained to the Adopter's reasonably anticipated production run rate. There will be no refunds for unused Keys or SmartRight Labels.

**2. REVOCATION AND RENEWAL PROCEDURES****2.1 Revocation Procedures.**

(a) Request for Revocation. If the owner of the SmartRight Product containing the Key sought to be revoked has provided an Adopter with information sufficient to permit communications to be addressed to such person (the "Registered Owner"),

the Association, upon its own initiative, or at the request of a Fellow Content Participant, may request a Revocation of a Key or Keys by notifying the Registered Owner of the grounds upon which such Revocation is sought.

(b) Revocation by Consent. If (i) the owner of the SmartRight Product containing the key sought to be Revoked has not provided information sufficient to permit communications to be addressed to such owner, (ii) Revocation is requested by the Registered Owner, or (iii) such Registered Owner consents to a request by the Association, the Association shall Revoke the Keys which are the subject of the request without further proceedings.

(c) Procedure for Contested Revocation. Within thirty (30) days following issuance by the Association of a Request for Revocation, the Registered Owner of any SmartRight Product which is the subject of the Request may notify the Association of any objections to the request and the grounds therefore. Upon receipt of such objection, the Association shall take such measures as it deems appropriate to investigate and ascertain (a) whether grounds exist for Revocation and (b) whether such grounds constitute a sufficient threat to the integrity of the SmartRight System to justify the Revocation. If the Revocation was requested by an Eligible Content Participant, then such Content Participant will be consulted and permitted to participate in the investigation.

(d) Judicial Review. The determination to Revoke or Renew a Key or Renew any SmartRight Products shall be made solely in the discretion of the Association giving due regard to the interests of content owners, content distributors, adopters and device owners whose interests may be affected thereby, and shall be subject to review in accordance with the procedures set forth in Article 78 of the New York Civil Practice Law and Rules upon the grounds set forth in section 7803, subdivision 3 thereof.

**2.2 Renewal Procedures.** Upon its own initiative or upon the request of any third party whose rights have been adversely affected, the Association may implement a procedure for Renewal of one or more SmartRight Products by notifying all SmartRight Participants having an interest in such products of its intention to seek such Renewal and the grounds upon which Renewal is sought.

(a) Within thirty (30) days following issuance by the Association of a Request for Renewal, any SmartRight Participants may make a submission to the Association setting forth its views as to (i) whether grounds exist for Renewal, (ii) whether such grounds constitute a sufficient threat to the integrity of the SmartRight System to justify the Renewal and (iii) the appropriate allocation among the SmartRight Participants of the costs of implementing the Renewal and the manner in which such costs may be funded.

(b) Following the receipt of the submissions, the Association shall take such measures as it deems appropriate to investigate and to determine whether such Renewal is appropriate.

(c) The decision of the Association to implement or not to implement a renewal shall be final and all SmartRight Participants shall be bound thereby.

(d) Implementation of Renewal. The Association shall delay the implementation of any Renewal for a sufficient period of time to ensure a smooth transition from the old system to the Renewed system. During that period, all owners of SmartRight Products affected by the Renewal shall either be sent new SmartRight Smart Cards free of charge, or provided with the opportunity to acquire such cards free of charge at a location or locations established for that purpose, and any Certified Keys issued to Adopters who have not yet sold devices containing such keys, or to distributors or retailers of such devices who have not resold the devices to consumers, shall be replaced.

### 3. PROCEDURES FOR THIRD PARTY BENEFICIARY CLAIMS

3.1 Prior to initiating or instituting an action to enforce any Third Party Beneficiary Claim under Section 10.4 of the Adopters Agreement, the party seeking to make such claim (the "Third Party Beneficiary") shall provide the Authority notice and consultation reasonable under the circumstances regarding its proposed claim; provided that such consultation with the Authority shall not affect such party's discretion to commence an action.

3.2 Promptly upon commencement of any action based on a Third Party Beneficiary Claim, the Third Party Beneficiary shall provide the Authority with notice of the commencement of any Action based on a Third Party Beneficiary Claim (a "Claim Notice") and, upon the Authority's request, copies of material documents supporting the claim.

3.3 Within thirty (30) days following the receipt of a Claim Notice the Association and any Adopter may, at its option, join as an indispensable party to the action and Third-Party Beneficiary and the Defendant shall not object to, any motion to so join. Any judgment entered upon such claim relating to the interpretation or enforceability of any provision of this Agreement shall be binding on the Authority and any Adopters that failed to join such Beneficiary Claim as if they had joined such action.

3.4 The Authority shall cooperate reasonably with the parties to any Third Party Beneficiary Claim by providing appropriate and necessary information to the extent that such cooperation is consistent with the preservation of the integrity and security of SmartRight Technology and to the extent such cooperation does not involve release of Confidential Information to a party not subject to an agreement with the Authority to protect the confidentiality of such information.

3.5 Third Party Beneficiaries and Adopter shall not enter into any settlement that: (i) amends any material term of any Adopter Agreement or Associate Founder Agreement; (ii) has an adverse effect on the integrity, performance and/or security of SmartRight Technology or on the operation of SmartRight™ Technology with respect to

protecting Commercial Audiovisual Content from any unauthorized output, transmission, interception or copying, or (iii) affects any of the rights of the Authority or its Licensors in and to SmartRight Technology or any intellectual property right embodied therein, unless the Authority shall have provided prior written consent thereto.

3.6 Nothing contained in these third party beneficiary procedures is intended to limit remedies or relief available pursuant to statutory or other claims that any party may have independent of its rights as a beneficiary of the Adopters Agreement.

## **SMARTRIGHT ADOPTERS AGREEMENT**

### **EXHIBIT B**

#### **COMPLIANCE RULES EFFECTIVE JANUARY 1, 2004**

##### **INTRODUCTION**

1. **DEFINITIONS.** The following definitions shall apply to this Exhibit B. Where a capitalized term is used but not otherwise defined in this Exhibit B, the meaning ascribed thereto elsewhere in the Agreement shall apply.

1.1 “Acquisition Device” means a SmartRight Product capable of receiving Conditional Access Content and/or Unencrypted Digital Terrestrial Broadcast Content.

1.2 “Add-in Device” means a SmartRight Product, such as a Computer bus card, that passes content to another product other than where such product passes, or directs such content to be passed to an output (e.g. where a demodulator add-in card in a personal computer passes such content to an associated software application installed in the same computer).

1.3 “Authorized Digital Protection Technology” means SmartRight Technology or another technology approved by the United States Federal Communications Commission pursuant to 73 C.F.R. §9008.

1.4 “Broadcast Flag” means the Redistribution Control descriptor (rc\_descriptor()) described in ATSC Standard A/65B: “Program and System Information Protocol for Terrestrial Broadcast and Cable.

1.5 “Combination Device” means a SmartRight Product which can perform the functions of an Acquisition Device and a Presentation Device.

1.6 “Commercial Audiovisual Content” shall mean audiovisual works, as defined in section 101 of the United States Copyright Act, which are (a) not created by the user of the Licensed Product and (b) offered for transmission, delivery or distribution, either generally or on demand, to subscribers or purchasers or the public at large, or otherwise for commercial purposes, not uniquely to an individual or a small, private group.

1.7 “Authorized Access Control Method” means any commercially adopted technological method or system which effectively controls access to Commercial Audiovisual Content, such as SmartRight, DTCP, CSS, Digicypher, Harmony, DBS and other

commercially-adopted access control technology, including digitally-controlled analog scrambling systems, whether now or hereafter in commercial use.

1.8 “Computer Product” shall mean a product which is designed for or permits the end user to install a wide variety of commercially available software applications, including applications, such as a personal computer, handheld “Personal Digital Assistants,” and the like and further including subsystems of such a product, such as a graphics card.

1.9 “Computer Monitor Output” means a connector for an analog or digital monitor typically found and associated with a Computer Product and which carries uncompressed analog and/or digital video signals. The term expressly includes those outputs known as VGA, SVGA and XGA, DVI outputs of devices manufactured on or prior to December 31, 2005 and various non-standardized digital monitor connections that were widely implemented as of May 1, 2002. The term expressly does not include such typical consumer electronics connectors as NTSC, PAL, SECAM, SCART, YPrPb, S-Video and Consumer RGB, whether or not such connectors are found on any Computer Product.

1.10 “Conditional Access Content” means Commercial Audiovisual Content delivered to an Acquisition Device through a Conditional Access Delivery Method.

1.11 “Conditional Access Delivery Method” shall mean any medium or service which employs an Authorized Access Control Method. Without limitation, “Conditional Access Delivery Methods” include Prerecorded Media, Pay Television Transmission; Pay-Per-View; Video-on-Demand; Subscription-on-Demand and Non-Premium Subscription Television, but shall not include content received through retransmission of a broadcast transmission (i.e., an over-the-air transmission for reception by the general public using radio frequencies allocated for that purpose) that, substantially simultaneously, is made by a terrestrial television broadcast station located within the country or territory in which the entity further transmitting such broadcast transmission also is located, where such broadcast transmission is not subject to a Commercially-Adopted Access Control Method (e.g., is broadcast in the clear and supported by advertising revenues or government mandated fees, without any other charge to members of the public receiving such broadcasts), regardless of whether such entity subjects such further transmission to an access control method. Notwithstanding the foregoing, Conditional Access Delivery Content shall include any service, Program, or schedule or group of Programs, that both (a) was primarily authored in a format with a resolution equal to or greater than 1000i or 700p (“High Definition”) and (b) is transmitted via a Commercially-Adopted Access Control Method in High Definition, provided that such service, Program, or schedule or group of Programs, is not, substantially simultaneously, transmitted in High Definition by a terrestrial broadcast station located within the same country or territory as Unencrypted Digital Terrestrial Broadcast Content.

1.12 “Consensus Watermark” shall mean a watermark technology designated as the “Consensus Watermark” by the Authority.

1.13 “Constrained Image” shall mean an image operating in a mode compatible with the Digital Visual Interface (DVI) Rev. 1.0 Specification as an image having the visual equivalent of no more than 350,000 pixels per frame (e.g., an image with resolution of 720 pixels by 480 pixels for a 4:3 aspect ratio), and 30 frames per second. A Constrained Image may be attained by reducing resolution, for example, by discarding, dithering, or averaging pixels to obtain the specified value. A Constrained Image can be displayed using video processing techniques such as line doubling or sharpening to improve the perceived quality of the image. By way of example, a Constrained Image may be stretched or doubled, and displayed full-screen, on a 1000-line monitor.

1.14 “Copy Freely” refers to Commercial Audiovisual Content which, as set out in the Specification, has been encoded by an Authorized Access Control Method so that copy control is not asserted, but which remains subject to the rights of the copyright owner.

1.15 “Copy Once” refers to Commercial Audiovisual Content which, as set out in the Specification, has been encoded by an Authorized Access Control Method as “Copy Once” indicating that only one generation of copies may be made of it following decryption.

1.16 “Copy Never” refers to Commercial Audiovisual Content which, as set in the Specification, has been encoded by an Authorized Access Control Method so that no copying is permitted following decryption.

1.17 “Copyright Watermark” shall mean the watermark technology designated in the Specification as the “Copyright Watermark.”

1.18 “Covered Demodulator Product” means an Acquisition Device or other product that is required under 47 CFR §§ 73.9002(a)(1) or 73.9002(b)(1) to comply with the Demodulator Compliance Requirements, and to be manufactured in accordance with the Demodulator Robustness Requirements of 73 CFR 9007.

1.19 “Decrypted SmartRight Content” means SmartRight Content that has been decrypted by a Presentation Device.

1.20 “Designated Watermarks” means the Copyright Watermark and, 18 months following its designation by the Authority, the Consensus Watermark.

1.21 “Digital Rights Management Method” means a technological measure that effectively controls access to a copyrighted work.

1.22 “Encrypted SmartRight Content” means SmartRight Content that has not been decrypted by a Presentation Device.

1.23 “EIT” means the Event Information Table as defined in ATSC Standard A/65B: “Program and System Information Protocol for Terrestrial Broadcast and Cable.”

1.24 “EPN Encoded Content” means SmartRight Content for which the associated EPN Data Field is set as described in the Specifications to indicate that copy control restrictions are not asserted with respect to such content (“EPN” stands for “Encryption Plus Non-assertion”).

1.25 “EPN Field” shall mean the field or bits, described in the Specification, used to indicate that Commercial Audiovisual Content is to be protected using SmartRight, the SmartRight Usage State to be applied to such content and, optionally, an Outbound Usage State.

1.26 “High Definition Analog Form” shall mean a format that is an analog video signal which has a resolution greater than a Constrained Image.

1.27 “High Definition Analog Output” shall mean an output capable of transmitting Commercial Audiovisual Content in High Definition Analog Form.

1.28 “Image Constraint Token” shall mean the field or bits, as described in the Specification, used to trigger the output of a “Constrained Image” in Authorized Access Control Methods.

1.29 “Marked Content” means (a) Unencrypted Digital Terrestrial Broadcast Content for which an Acquisition Device has received, demodulated and either the EIT or the PMT inspected and determined the Broadcast Flag to be present or (b) Unencrypted SmartRight Content which was previously determined by an Acquisition Device to have been Marked Content.

1.30 “Non-Premium Subscription Television” shall mean a Conditional Access Delivery of a service, or schedule or group of Programs (which may be offered for sale together with other services, or schedule or group of Programs), for which subscribers are charged a subscription fee for the reception or viewing of the programming contained therein, other than Pay Television Transmission and Subscription-on-Demand. By way of example, “basic cable service” and “extended basic cable service” in the United States (other than such programming contained therein that does not fall within the definition of Conditional Access Delivery) are “Non-Premium Subscription Television.”

1.31 “Outbound Usage State” is the usage state that is applied by a Presentation Device to determine the output rules applicable to the exportation of Decrypted SmartRight Content to other Control Access Systems. The permitted Output Usage States are Copy Freely, Copy Once, Copy Never and Output Forbidden.

1.32 “Output Forbidden” refers to the Outbound Usage State which specifies that Decrypted SmartRight Content may not be passed to any output.

1.33 “Pay-Per-View” shall mean a delivery of a single Program or a specified group of Programs, as to which each such single Program is generally uninterrupted by Commercial Advertising Messages and for which recipients are charged a separate fee for each Program or specified group of Programs. The term “Pay-Per-View” shall also in-



clude delivery of a single Program as described above for which multiple start times are made available at time intervals which are less than the running time of such Program as a whole. If a given delivery qualifies both as Pay-Per-View and a Pay Television Transmission, then, for purposes of this Agreement, such delivery shall be deemed Pay-Per-View rather than a Pay Television Transmission.

1.34 “Pay Television Transmission” shall mean a transmission of a service or schedule of Programs, as to which each individual Program is generally uninterrupted by Commercial Advertising Messages and for which service or schedule of Programs subscribing viewers are charged a periodic subscription fee, such as on a monthly basis, for the reception of such programming delivered by such service whether separately or together with other services or programming, during the specified viewing period covered by such fee. If a given delivery qualifies both as a Pay Television Transmission and Pay-Per-View, Video-on-Demand, or Subscription-on-Demand then, for purposes of this Agreement, such delivery shall be deemed Pay-Per-View, Video-on-Demand or Subscription-on-Demand rather than a Pay Television Transmission.

1.35 “Peripheral TSP Product” means a product that is capable of accessing in usable form Unscreened Content or Marked Content passed to such product via a Robust Method where the manufacturer of such product has committed in writing in accordance with § 73.9002(c) that such product will comply with the Demodulator Compliance Requirements and be manufactured in accordance with the Demodulator Robustness Requirements.

1.36 “Output Categories” mean the categories of video output for which Outbound Usage States may be specified for Decrypted SmartRight Content exported to another Authorized Access Control Method. The Output Categories which may be specified for Decrypted SmartRight Content include (a) standard definition analog output, (b) high definition analog output, (c) uncompressed digital output and (d) compressed digital output.

1.37 “PMT” means Program Map Table as defined in International Standard ISO/IEC 13818-1:2000(E): “Information Technology – Generic Coding of Moving Pictures and Associated Audio Information: Systems”.

1.38 “Prerecorded Media” shall mean the delivery of one or more Programs, in prerecorded and encrypted or scrambled form, on packaged media, such as DVD discs.

1.39 “Presentation Device” means a SmartRight Product capable of decrypting Encrypted SmartRight Content.

1.40 “Private Copy” refers to the SmartRight Usage State specifying that such content may be freely copied, but may only be displayed by Presentation Devices within a particular Personal Private Network.

1.41 “Program” shall mean any work of Commercial Audiovisual Content.

1.42 “Retention State Field” shall mean the field or bits, as described in the Specification, used to specify the time period during which a Session Key can be decrypted by a Presentation Device.

1.43 “Robust Method” means a data path which complies with Section 2 of the Compliance Rules.

1.44 “Session Key” means a Key generated by a Converter Card for decrypting the LECM of View Only SmartRight Content. A Session Key is stored solely in the converter card which converted the content during the period designated in the Retention State Field.

1.45 “SmartRight Usage State” means the usage state that is specified in the LECM for Encrypted SmartRight Content. The permitted SmartRight Usage states are Copy Freely, Private Copy and View Only.

1.46 “Standard Definition Analog Output” means an NTSC, YUV, SECAM, PAL, or consumer RGB format analog output (including an S-video output for the listed formats) that carries uncompressed video signals with a resolution less than or equal to a Constrained Image.

1.47 “Storage Only Device” means a SmartRight Product which can store or record Encrypted SmartRight Content, but which does not perform the functions of an Acquisition Device or a Presentation Device.

1.48 “Subscription-on-Demand” shall mean the delivery of a single Program or a specified group of Programs for which (i) a subscriber is able, at his or her discretion, to select the time for commencement of exhibition thereof; (ii) where each such single Program is generally uninterrupted by Commercial Advertising Messages; and (iii) for which Program or specified group of Programs subscribing viewers are charged a periodic subscription fee for the reception of programming delivered by such service during the specified viewing period covered by the fee. In the event a given delivery of a Program qualifies both as a Pay Television Transmission and Subscription-on-Demand, then for purposes of this Agreement, such delivery shall be deemed Subscription-on-Demand rather than a Pay Television Transmission.

1.49 “Transitory Image” shall mean data which has been stored temporarily for the sole purpose of enabling the immediate display of content but which (a) does not persist materially after the content has been displayed and (b) is not stored in a way which permits copying or storing of such data for other purposes.

1.50 “Unencrypted Digital Terrestrial Broadcast Content” means Commercial Audiovisual Content contained in the signal broadcast by a digital television station without encrypting or otherwise making the content available through a technical means of conditional access, and includes such content when retransmitted in unencrypted digital form.

1.51 “Unscreened Content” means, with respect to an Acquisition Device, Unencrypted Digital Terrestrial Broadcast Content that such product either (1) received and demodulated and for which such product has inspected neither the EIT nor the PMT for the Broadcast Flag or (2) has received via a Robust Method and accessed in usable form, and for which such product has inspected neither the EIT nor the PMT for the Broadcast Flag and has not determined through information robustly conveyed with such content another Covered Demodulator Product had previously so screened such content and determined the Broadcast Flag to be present; provided, however, that, with respect to a Covered Demodulator Product, “Unscreened Content” shall not include content that has been passed from such product pursuant to Section 2.1 of these rules.

1.52 “User Accessible Bus” means a data bus that is designed for end user upgrades or access, such as an implementation of a smartcard interface, PCMCIA, Cardbus, or PCI that has standard sockets or otherwise readily facilitates end user access. A “User Accessible Bus” does not include memory buses, CPU buses, or similar portions of a device's internal architecture that do not permit access to content in a form usable by end users. This Definition should be interpreted and applied so as to allow Adopter to design and manufacture its products to incorporate means, such as test points, used by Adopter or professionals to analyze or repair products; but not to provide a pretext for inducing consumers to obtain ready and unobstructed access to internal analog connectors. Without limiting the foregoing, an internal analog connector shall be presumed to not “readily facilitate end user access” if (i) such connector and the video signal formats or levels of signals provided to such connector, are of a type not generally compatible with the accessible connections on consumer products, (ii) such access would create a risk of product damage, or (iii) such access would result in physical evidence that such access had occurred and would void any product warranty.

“Video-on-Demand” shall mean a delivery of a single Program or a specified group of Programs for which (i) each such individual Program is generally uninterrupted by Commercial Advertising Messages; (ii) recipients are charged a separate fee for each such single Program or specified group of Programs; and (iii) a recipient is able, at his or her discretion, to select the time for commencement of exhibition of such individual Program or specified group of Programs. In the event a delivery qualifies as both Video-on-Demand and a Pay Television Transmission, then for purposes of this Agreement, such delivery shall be deemed Video-on-Demand.

1.53 “View Only” refers to Commercial Audiovisual Content which, as set out in the Specification, has been encoded as “View Only.”

## 2. COMPLIANCE RULES APPLICABLE TO UNENCRYPTED DIGITAL TERRESTRIAL BROADCAST CONTENT.

### 2.1 Unscreened Content.

(a) **Output of Unscreened Content.** A SmartRight Product shall not pass, or direct to be passed, Unscreened Content to any output except:

- (i) to an analog output;
  - (ii) to an 8-VSB, 16-VSB, 64-QAM or 256-QAM modulated output, provided that the Broadcast Flag is retained in the both the EIT and PMT;
  - (iii) to a digital output protected by an Authorized Digital Output Protection Technology authorized for use with Unscreened Content, in accordance with any applicable obligations established as a part of its approval pursuant to 47 CFR §73.9008;
  - (iv) where the stream containing such content has not been altered following demodulation and such Covered Demodulator Product outputs, or directs to be output, such content to a Peripheral TSP Product solely within the home or other, similar local environment, using a Robust Method;
  - (v) where such product outputs, or directs to be output, such content for the purpose of making a recording of such content pursuant to paragraph (b)(ii) of this section, where such content is protected by the corresponding recording method; or
  - (vi) where such Covered Demodulator Product is incorporated into a Computer Product and passes, or directs to be passed, such content to an unprotected output operating in a mode compatible with the Digital Visual Interface (DVI) Rev. 1.0 Specification as an image having the visual equivalent of no more than 350,000 pixels per frame (e.g. an image with resolution of 720 x 480 pixels for a 4:3 (nonsquare pixel) aspect ratio), and 30 frames per second. Such an image may be attained by reducing resolution, such as by discarding, dithering or averaging pixels to obtain the specified value, and can be displayed using video processing techniques such as line doubling or sharpening to improve the perceived quality of the image.
- (b) **Recording of Unscreened Content.** SmartRight Products shall not record or cause the recording of Unscreened Content except by:
- (i) a method that effectively and uniquely associates such recording with a single Device (using cryptographic protocol or other effective means) so that such recording cannot be accessed in usable form by another product except where the content of such recording is passed to another product as permitted under these Rules or
  - (ii) an Authorized Recording Method approved by the United States Federal Communications Commission for use with Unscreened Content pursuant to 47 C.F.R. § 73.9008 (provided that for recordings made on removable media, only Authorized Recording Methods expressly approved pursuant to § 73.9008 for use in connection with removable media may be used).
- (c) Paragraph (b) of this section does not impose restrictions regarding the storage of Unscreened Content as a Transitory Image.

## 2.2 Marked Content

(a) **Output of Marked Content.** A SmartRight Product shall not pass, or direct to be passed, Marked Content to any output except

- (i) to an analog output;
- (ii) to an 8-VSB, 16-VSB, 64-QAM or 256-QAM modulated output, provided that the Broadcast Flag is retained in the both the EIT and PMT;
- (iii) to a digital output protected by an Authorized Digital Output Protection Technology, in accordance with any applicable obligations established as a part of its approval pursuant to § 73.9008;
- (iv) as Private Copy Encrypted SmartRight Content;
- (v) where such product outputs, or directs to be output, such content for the purpose of making a recording of such content pursuant to paragraph (b)(2) of this section, where such content is protected by the corresponding recording method; or
- (vi) where such Product is incorporated into a Computer Product and passes, or directs to be passed, such content to an unprotected output operating in a mode compatible with the Digital Visual Interface (DVI) Rev. 1.0 Specification as an image having the visual equivalent of no more than 350,000 pixels per frame (e.g., an image with resolution of 720 x 480 pixels for a 4:3 (nonsquare pixel) aspect ratio), and 30 frames per second. Such an image may be attained by reducing resolution, such as by discarding, dithering or averaging pixels to obtain the specified value, and can be displayed using video processing techniques such as line doubling or sharpening to improve the perceived quality of the image.

(b) **Recording of Marked Content.** A SmartRight Product shall not record or cause the recording of Marked Content in digital form unless such recording is made using one of the following methods:

- (i) as Encrypted SmartRight Content, or using another method that effectively and uniquely associates such recording with a single Covered Demodulator Product (using a cryptographic protocol or other effective means) so that such recording cannot be accessed in usable form by another product except where the content of such recording is passed to another product as permitted under this subpart or
- (ii) an Authorized Recording Method in accordance with any applicable obligations established as a part of its approval by the FCC pursuant to 47 CFR §73.9008 (provided that for recordings made on removable media, only Authorized Recording Methods expressly approved by the FCC pursuant to 47 CFR §73.9008 for use in connection with removable media may be used).

(c) Paragraph (b) of this section does not impose restrictions regarding the storage of Marked Content as a Transitory Image.

**2.3 Output Restrictions on Audio.** Except as otherwise provided in §§2.1(a) or 2.2(a), Covered Demodulator Products shall not output the audio portions of Unscreened Content or of Marked Content in digital form except in compressed audio format (such as AC3) or in Linear PCM format in which the transmitted information is sampled at no more than 48 kHz and no more than 16 bits/sample.

**2.4 Add-In Devices.** Where an Add-In Device passes Unscreened Content or Marked Content to another product, other than where such Covered Demodulator Product passes, or directs such content to be passed to an output (e.g., where a demodulator add-in card in a personal computer passes such content to an associated software application installed in the same computer), it shall pass such content:

(a) using a Robust Method; or

(b) as Encrypted SmartRight Content or using Authorized Digital Output Protection Technology authorized for such content in accordance with any applicable obligations established as a part of its approval by the FCC pursuant to 47 CFR §73.9008. Neither Unscreened Content nor Marked Content may be so passed in unencrypted, compressed form via a User Accessible Bus.

**2.5 Unmarked Content.** SmartRight Products shall place no restrictions on the output, recording or display of Unencrypted Terrestrial Broadcast Content which is not Unscreened Content or Marked Content.

### 3. COMPLIANCE RULES APPLICABLE TO ACQUISITION DEVICES.

**3.1 Communications Capability.** All Acquisition Devices shall have a digital communications port communicate over a digital network with other SmartRight Products using a protocol in accordance with the Specification.

**3.2 Inspection of Unencrypted Digital Terrestrial Broadcast Content for Broadcast Flag.** All Acquisition devices which (a) receive and demodulate Unencrypted Digital Terrestrial Broadcast Content, or have received such content in usable form via a Robust Method from a Covered Demodulator Product shall inspect either the EIT or the PMT of all Unencrypted Digital Terrestrial Broadcast Content prior to any digital output to determine the presence of the Broadcast Flag. In the event such inspection determines that the Broadcast Flag is present, the Marked Content shall be converted by the Acquisition Device into Private Copy Encrypted SmartRight Content.

#### **3.3 Inspection of Conditional Access Content.**

(a) All Acquisition Devices which receive Conditional Access Content shall inspect such content prior to output to determine the presence of an EPN Field and the contents thereof.

(b) Following the implementation of the Consensus Watermark, as provided in Section 8.2(i), all acquisition devices which receive unencrypted Conditional Access Content shall inspect such content prior to any output to determine the existence of a Consensus Watermark.

### 3.4 Conversion of SmartRight Content.

(a) Marked Content and unencrypted Conditional Access Content containing an EPN field or a Consensus Watermark will be encrypted by the Acquisition Device. The encryption will preserve the Broadcast Flag, the Designated Watermarks, and any information included in the content for use by other Access Control Methods.

(b) The Converter Card will generate an LECM to be packaged with the Encrypted Content by the Acquisition Device in accordance with the Specification which shall contain the information required by authorized Presentation Devices to decrypt the content and enforce the Usage States associated therewith, including whether the content was Marked Content and the appropriate SmartRight Usage State and any Output Usage State designated by the EPN Field.

(c) The LECM for Copy Freely SmartRight Content shall not be encrypted.

(d) The LECM for Private Copy and View Only SmartRight Content shall be encrypted by a Converter Card connected to the PPN using the Network Key applicable to the PPN with which the Device is associated, as defined by Specifications.

(e) In addition, The LECM for View Only SmartRight Content shall be super-encrypted using a Session Key generated by a Converter Card which is not stored with the SmartRight Content but is retained in the Converter Card only for the period of time designated in the Retention State Field.

### 3.5 Output Restrictions.

(a) **SmartRight Content.** SmartRight Content may not be output by any Acquisition Device except to a digital output in the form of Encrypted SmartRight Content.

(b) **Compatibility with Other Systems.** Nothing in the Specification or these Compliance Rules shall interfere with or prevent any Acquisition Device from complying with any restrictions on the output Controlled Access Content imposed by any other Access Control Method.

(c) **Consensus Watermark.** Acquisition Devices will comply with the rules applicable to unscrambled content containing the Consensus Watermark as provided in Section 8.2 below.

### 3.6 Storage and Recording Restrictions.

(a) **SmartRight Content.** An Acquisition Device shall not record or cause the recording of SmartRight Content except Encrypted SmartRight Content may be recorded in digital form such that only an authorized Presentation Device can decrypt the content.

(b) **Non-SmartRight Controlled Access Content.** Nothing in the Specification or these Compliance Rules shall interfere with or prevent any Acquisition Device from complying with any restrictions on storage or recording of Controlled Access Content imposed by any other Access Control Method.

(c) **Internal Storage.** The restrictions imposed by this section do not apply to internal storage of content as a Transitory Image.

#### 4. COMPLIANCE RULES APPLICABLE TO PRESENTATION DEVICES

4.1 **Communications Capability.** All Presentation Devices shall have a digital communications port which permits it to communicate over a digital network with other SmartRight Products in accordance with the Specification.

##### 4.2 **Key Generation.**

###### (a) **Network Keys.**

(i) Upon connection to a PPN, a Presentation Device will communicate with any other Presentation Device, as provided in the Specification, to determine whether a Network Key has been generated.

(ii) If no other Presentation device is connected to the PPN, the Terminal Module will generate and store a new Network Key.

(iii) If other Presentation Devices are connected to the PPN and the Maximum Network Size has not previously been reached, the Terminal Module will store the existing Network Key.

(iv) No more than one Network Key may be stored in any Terminal Module. Once a Network Key has been stored in a Terminal Module, it will not store a new Network Key until the previous Key has been erased.

##### 4.3 **Decryption of SmartRight Content.**

(a) **Copy Freely.** All Presentation Devices may decrypt Copy Freely Encrypted SmartRight Content.

(b) **Private Copy.** All Private Copy SmartRight Content shall be decrypted using the Network Key applicable to the PPN with which the Presentation Device is associated. Any View Only or Private Copy SmartRight Content packaged with a different Network Key shall not be processed.



(c) **View Only.** View Only SmartRight Content shall be decrypted using a Session Key stored in an Acquisition Device which encrypted the content within the time period specified in the Retention State Field. Any View Only SmartRight Content for which a Session Key is not stored in an Acquisition Device connected to the PPN shall not be processed.

(d) **Preservation of Control Information.** The decryption of SmartRight Content by a Presentation Device shall preserve the Broadcast Flag and any information included in the content for use by other Access Control Methods.

#### 4.4 **Compatibility with other Protection Systems.**

(a) Nothing in the Specification or these Rules shall prohibit or interfere with the ability of a Presentation Device to receive or process information in compliance with any other Access Control Method.

(b) All Presentation Devices capable of displaying a video image with resolution greater than a Constrained Image shall respond to the Constrained Image Token.

#### 4.5 **Output Control of Decrypted SmartRight Content.**

(a) **Marked Content.** Marked Content which has been decrypted by a Presentation Device may not be passed to any output except as authorized by Section 2.2.

(b) **Conditional Access Content.**

(i) A Presentation Device shall not pass the Decrypted SmartRight Content other than Marked Content to any output except as follows:

(1) Presentation Devices that are not configured to export content to other Authorized Access Control Methods by a Robust Method may only output Decrypted SmartRight Content with a Copy Freely Outbound Usage State applicable to such Output Category. For example, Decrypted SmartRight Content with an Outbound User State of Copy Freely for Standard Definition Analog Output but as Copy Never for all other Outputs may only be passed to a Standard Definition Analog Output.

(2) **Assigning Output Usage States.** Presentation Device configured to export Decrypted SmartRight Content to another Authorized Access Control Method shall assign an Outbound Usage State corresponding to the SmartRight Usage State to any Decrypted SmartRight Content that was not assigned an Outbound Usage State by the EPN Field, as follows:

SmartRight Usage State	Outbound Usage State
Copy Freely	Copy Freely
Private Copy	Copy Never

View Only	Copy Never
-----------	------------

(ii) Presentation Devices configured to export content to other Authorized Access Control Methods may only direct output of Conditional Access Content to an Output Category which provides a level of protection sufficient to provide the at least same degree of protection specified by the Outbound Usage State for that Output Category. If the Authorized Access Control Method does not provide the same level of protection designated by the Outbound Usage State, but provides a higher level of protection, the content may be exported to that system with a Usage State requiring that higher level of protection. For example, content designated as Copy Never for uncompressed digital output and Copy Once for all other Output Categories may be output to a DVI or DTCP device but may not be output to a system that does not provide any protection for analog output. Such content may also be designated as Copy Never and output to an Authorized Access Control Method that does not provide Copy Once protection to all Output Categories, but provides Copy Never protection. Without limiting the generality of the foregoing, the following rules to specific Output Categories.

(iii) **Digital Video Output**

(1) **DTCP.** When passing Decrypted SmartRight Content to an output protected by DTCP, a Presentation Device shall (a) carry any DTCP System Renewability Messages delivered in association with such content to the DTCP Source Function, (b) set the APS field of the DTCP Descriptor in accordance with APSTB field of the corresponding Real-time Data Information (RDI) pack, (c) set the EPN field of the DTCP Descriptor to 0 (EPN-Asserted), or to 1 (EPN-unasserted) and (d) set fields of the DTCP Descriptor to the appropriate binary values for the Outbound Usage State as determined by the SmartRight EPN Field or Section.

(2) **HDCP.** When passing Decrypted SmartRight Content to an output protected by HDCP, a Presentation Device shall (a) carry any HDCP System Renewability Message delivered in association with such content to the HDCP Source Function and (b) verify that the HDCP Source Function is engaged and able to deliver protected content, which means (i) HDCP encryption is operational on such output, (ii) processing of the valid received System Renewability Message associated with content, if any, has occurred as defined in the HDCP Specification; and (iii) there is no HDCP Display Device or Repeater on such output whose Key Selection Vector is in such System Renewability Message. Capitalized terms used in the foregoing but not otherwise defined in the Specifications or this Agreement shall have the meaning set forth in the HDCP Specification and HDCP Adopter Agreement.

(iv) **Digital Audio Outputs.** A Presentation Device may pass the audio portion of Decrypted SmartRight Content to a digital output other than an Authorized Access Control Method provided that such content is in compressed audio format (such as AC3) or in Linear PCM format in which the transmitted information is sampled at no more than 48 kHz and no more than 16 bits. Adopter is cautioned and notified that this requirement may be revised.

(v) **Computer Monitor Outputs.** A Presentation Device operating as an internal or peripheral component of a Computer Product may pass Decrypted SmartRight Content to a Computer Monitor Output.

(vi) **Standard Definition Analog Output.** A Presentation Device may pass the video portion of Decrypted SmartRight Conditional Access Content to a Standard Definition Analog Video output, provided that for such content that is not EPN Encoded Content, it generates copy control signals according to the APSTB and CGMS fields of the corresponding Real-time Data Information (RDI) pack, using the following copy control systems:

(1) For an NTSC analog output, however transmitted, Automatic Gain Control and Colorstripe according to the APSTB field, and CGMS-A according to the CGMS field;

(2) For a PAL, SECAM or YUV analog output, Automatic Gain Control according to the APSTB field, and CGMS-A according to the CGMS field (note that “YUV” as used herein means a component video output comprised of a luminance signal (Y) and two color difference signal (U and V) and specifically includes the following component video signals (Y, Pb, Pr), (Y, Cb, Cr), (Y, Db, Dr), and (Y, B-Y, R-Y));

(3) For a 480p progressive scan analog output, Automatic Gain Control according to the APSTB field, and CGMS-A according to the CGMS field; and

(4) For an SCART connector, Automatic Gain Control specifications for the PAL and SECAM signal carried by that connector, provided that the connector must be configured so that the component signal carried by the connector must always be accompanied by a composite signal and such composite signal must provide the only synchronization reference for the component signal.

(5) Notwithstanding the foregoing, the requirements to comply with the CGMS-A specification set forth in this Section shall not apply to a Presentation Device operating as an internal or peripheral component of a Computer Product.

(vii) **High Definition Analog Output.** A Presentation Device may pass the video portion of Decrypted SmartRight Conditional Access Content to a High Definition Analog Video output, provided that for such content that is not EPN Encoded Content, it generates copy control signals sufficient to comply with the designated Output Usage State in accordance with 4.5(b)(ii) above.

(viii) **Analog Audio Outputs.** A Participating Video Player may pass the audio portion of Decrypted CPRM Video Content to an analog audio output without restriction.

4.6 **Recording and Storage of Decrypted Smart Right Content.** Decrypted SmartRight Content may not be recorded or stored by a Presentation Device except as follows:

4.7 **Marked Content** Recording and Storage of Marked Content shall be governed by Section 2.2(b).

4.8 **Conditional Access Content.**

(a) Any storage of decrypted View Only SmartRight Content shall be for a period no greater than the time the set out in the Retention State Field and shall be removed from storage following the expiration of that time.

(i) Decrypted Conditional Access Content other than View Only Content may be recorded pursuant to a recording method which permits no greater usage than would be allowed by an output authorized by section 4.5.

## 5. COMPLIANCE RULES APPLICABLE TO COMBINATION DEVICES

Combination Devices shall comply with all Compliance Rules set forth in Articles 2, 3, 4, 7 and 8 of these Rules other than Sections 3.5(a) and 3.6(a).

## 6. COMPLIANCE RULES APPLICABLE TO STORAGE ONLY DEVICES

Storage Only Devices shall comply with all Compliance Rules set forth in Articles 2, 3, 7 and 8 of these Rules other than Sections 3.1, 3.2, 3.3, and 3.4.

## 7. PROTECTION AGAINST INTERNET TRANSMISSION AND “BOOTLEG” COPIES

7.1 **Proximity Control for SmartRight Content.** All SmartRight Products shall apply the proximity control provisions of the Specification to determine whether SmartRight Content received through a digital communications port was transmitted through the public internet. SmartRight Content which is determined to have been transmitted over the public internet without authorization shall not be decrypted, stored, recorded, displayed or output by the Device.

7.2 **Non-SmartRight Content.** All SmartRight Products shall inspect any digital audiovisual content other than Encrypted SmartRight Content received in any manner other than by a Conditional Access Delivery Method or as Unencrypted Digital Terrestrial Broadcast Content for the presence of an EPN Field and the Broadcast Flag. Any such content containing the broadcast flag, or designated other than as Copy Freely by the EPN Field, shall not be decrypted, stored, recorded, displayed or output by the Device.

7.3 **Consensus Watermark.** Following the implementation of the Consensus Watermark, as provided in Section 8.2(i), all SmartRight Products shall inspect any digital audiovisual content other than Encrypted SmartRight Content received in any manner other than by a Conditional Access Delivery Method or as Unencrypted Digital Terrestrial Broadcast Content for the presence of the Consensus Watermark. Any such content designated Copy Never, or the equivalent, shall not be stored or recorded by the Device

## 8. CONSENSUS AND COPYRIGHT WATERMARK IMPLEMENTATION

8.1 **Pre-Implementation Protection of the Consensus Watermark.** Commencing on the date that the Authority identifies the Consensus Watermark and the Copyright Watermark, Adopter:

(i) Shall, when selecting among technological implementations for product features of Licensed Products designed after such date, take commercially reasonable care (taking into consideration the reasonableness of the costs of implementation, as well as the comparability of their technical characteristics, of applicable commercial terms and conditions, and of their impact on Decrypted Data and on the effectiveness and visibility of the Consensus Watermark) that SmartRight Products and components thereof do not strip, interfere with or obscure the Consensus Watermark;

(ii) Shall not design new products or components thereof for which the primary purpose is to strip, interfere with or obscure the Consensus Watermark; and

(iii) Shall not knowingly promote or knowingly advertise or knowingly cooperate in the promotion or advertising of products or components thereof for the purpose of stripping, interfering with or obscuring the Consensus Watermark.

8.2 **Protection of Designated Watermarks.** The following provisions are applicable to the Copyright Watermark and, with respect to all SmartRight Products manufactured within 18 months following its designation, to the Consensus Watermark:

(i) Acquisition Devices shall be designed to inspect unencrypted Conditional Access Content for the presence of a Consensus Watermark and shall convert such content to Encrypted Smart Right Content with the appropriate SmartRight Usage State and Outbound Usage State;

(ii) Presentation Devices shall not process any content containing a Copyright Watermark unless such content is received in the form of Encrypted SmartRight Content;

(iii) Adopter shall not produce Licensed Products or components thereof for which the primary purpose is to strip, interfere with or obscure a Designated Watermarks; and

(iv) Adopter shall not knowingly distribute or knowingly cooperate in distribution of Licensed Products or components thereof for the purpose of stripping, interfering with or obscuring the Designated Watermarks.

(b) **Product Features.** This Article 8 shall not prohibit a Licensed Product or Licensed Component from incorporating legitimate features (i.e., zooming, scaling, cropping, picture-in-picture, compression, recompression, image overlays, overlap of windows in a graphical user interface, audio mixing and equalization, video mixing and keying, downsampling, upsampling, and line doubling, or conversion between widely-used formats for the transport, processing and display of audiovisual signals or data, such as between analog and digital formats and between PAL and NTSC or RGB and YUV formats, as well as other features as may be added to the foregoing list from time to time by the Authority by amendment to these Compliance Rules) that are not prohibited by law, and such features shall not be deemed to strip, interfere with or obscure the Designated Watermark, provided that (a) Adopter shall take commercially reasonable care that such features in a Licensed Product do not strip, obscure, or interfere with a Designated Watermark in Conditional Access Delivery Content received by such Licensed Product, and (b) Adopter shall not knowingly market or knowingly distribute, or knowingly cooperate in marketing or distributing, such Licensed Products or Licensed Components for the purpose of stripping, obscuring or interfering with a Designated Watermark in Conditional Access Delivery Content.

(c) Adopter is alerted that the requirements of this Article 8, and the declaration of the Consensus Watermark, may be rescinded by the Association if, during the two (2) year period immediately preceding the fourth anniversary of such declaration, the Consensus Watermark has not been implemented by major content providers in more than thirty-three percent (33%) of DVD discs of new theatrical motion pictures produced for DVD released by such providers in the United States of America and Canada during such period.

## EXHIBIT "C" ROBUSTNESS RULES

### 1. CONSTRUCTION

1.1 **Generally.** SmartRight Products as shipped shall meet the applicable Compliance Rules set forth in Exhibit B, and shall be manufactured in a manner clearly designed to effectively frustrate attempts to modify such Licensed Products to defeat the content protection requirements of SmartRight set forth in the Specification and Compliance Rules merely by using general-purpose tools or equipment that are widely available at a reasonable price, such as screwdrivers, jumpers, clips and soldering irons ("Widely Available Tools"), or using specialized electronic tools or specialized software tools that are widely available at a reasonable price, such as EEPROM readers and writers, debuggers or decompilers ("Specialized Tools"), other than devices or technologies whether Hardware or Software that are designed and made available for the specific purpose of bypassing or circumventing the protection technologies required by SmartRight ("Circumvention Devices").

1.2 **Defeating Functions.** Licensed Products shall not include:

- (a) (a) switches, buttons, jumpers or software equivalents thereof,
- (b) (b) specific traces that can be cut, or
- (c) (c) functions (including service menus and remote-control functions),

in each case by which the mandatory provisions of the Specification or the Compliance Rules, including the content protection technologies, analog protection systems, output protections, output restrictions, recording protections or recording limitations can be defeated, or by which Unscreened Content, Marked Content or Conditional Access Content (collectively "Protected Content") in such Licensed Products can be exposed to output, interception, retransmission or copying, in each case other than as permitted under this Agreement.

1.3 **Keep Secrets.** Licensed Products shall be manufactured in a manner that is clearly designed to effectively frustrate attempts to discover or reveal Keys and any other Highly Confidential Information.

1.4 **Robustness Checklist.** Before releasing any Licensed Product, Adopter must perform tests and analyses to assure compliance with these Robustness Rules. A Robustness Checklist is attached as Exhibit C-1 for the purpose of assisting Adopter in performing tests covering certain important aspects of these Robustness Rules. Inasmuch as the Robustness Checklist does not address all elements required for the manufacture of a Compliant product, Adopter is strongly advised to review carefully the Specification,

Compliance Rules (including, for avoidance of doubt, these Robustness Rules) so as to evaluate thoroughly both its testing procedures and the compliance of its Licensed Products. Adopter shall provide copies of the Specification, the Compliance Rules (including, for avoidance of doubt, these Robustness Rules) and the Robustness Checklist to its supervisors responsible for design and manufacture of Licensed Products.

## 2. **DATA PATHS.**

2.1 Unencrypted Content shall not be available on outputs other than those specified in the Compliance Rules.

2.2 Protected Content decrypted by an Add in Device shall not be present on a User Accessible Bus in analog or unencrypted, compressed form.

2.3 Protected Content with an Outbound Usage State restricting its output to exportation to another device employing an Authorized Access Control Method must be encrypted, compressed, encoded or otherwise output in accordance with the compliance rules of the destination Authorized Access Control Method applicable to data moving from one device to another.

3. **REVISIONS.** Adopter is alerted that these Robustness Rules may be revised in the future, upon notification by the Authority, to require that, when the Authority deems that it is technically feasible and commercially reasonable to do so, Licensed Products be clearly designed such that when uncompressed, Decrypted SmartRight Content is transmitted over a User Accessible Bus, such Decrypted SmartRight Content is made reasonably secure from unauthorized interception by use of means that can be defeated neither by using Widely Available Tools nor by using Specialized Tools, except with difficulty, other than Circumvention Devices. The level of difficulty applicable to Widely Available Tools is such that a typical consumer should not be able to use Widely Available Tools, with or without instruction, to intercept such Decrypted SmartRight Content without risk of serious damage to the product or personal injury. Adopter is further alerted that, when it is deemed technically feasible and reasonably practicable to do so, the Authority will revise these Robustness Rules to require that uncompressed Decrypted SmartRight Content will be re-encrypted or otherwise protected before it is transmitted over such buses.

3.1 **METHODS OF MAKING FUNCTIONS ROBUST.** Licensed Products shall be manufactured using at least the following techniques in a manner that is clearly designed to effectively frustrate attempts to defeat the content protection requirements set forth below.

3.2 **Distributed Functions.** Where Protected Content is delivered from one part of the Licensed Product to another, whether among integrated circuits, software modules, or otherwise or a combination thereof, the portions of the Licensed Product that perform authentication and decryption and the MPEG (or similar) decoder shall be designed and manufactured in a manner associated and otherwise integrated with each other such that data flowing in any usable form flowing between these portions of the Licensed



Product shall be reasonably secure from being intercepted or copied except as authorized by the Compliance Rules.

3.3 **Software.** Any portion of the Licensed Product that implements any of the content protection requirements of the Specification or the Compliance Rules by Software shall comply with all of the requirements forth in Sections 1 and 2 of this Exhibit C. For the purposes of these Robustness Rules, "Software" shall mean the implementation of the content protection requirements as to which this Agreement requires a Licensed Product to be compliant through any computer program code consisting of instructions or data, other than such instructions or data that are included in Hardware. Such implementations shall:

(a) **Keep Secrets.** Comply with Section 1.3 of this Exhibit C by a reasonable method including but not limited to: encryption, execution of a portion of the implementation in ring zero or supervisor mode, and/or embodiment in a secure physical implementation; and, in addition, in every case of implementation in Software, using techniques of obfuscation clearly designed to effectively disguise and hamper attempts to discover the approaches used.

(b) **Self-Checking for Unauthorized Modifications.** Be designed so as to perform self-checking of the integrity of its component parts such that unauthorized modifications will be expected to result in a failure of the implementation to provide the authorized authentication and/or decryption function. For the purpose of this provision, a "modification" includes any change in, or disturbance or invasion of, features or characteristics, or interruption of processing, relevant to Sections 1 and 2 of this Exhibit C. This provision requires at a minimum the use of "signed code" or more robust means of "tagging" operating throughout the code.

3.4 **Hardware.** Any portion of the Licensed Product that implements any of the content protection requirements of the Specification or the Compliance Rules by Hardware shall include all of the characteristics set forth in Sections 1 and 2 of this Exhibit C. For the purposes of these Robustness Rules, "Hardware" shall mean a physical device other than a SmartRight Smart Card, including a Licensed Component that implements any of the content protection requirements as to which this Agreement requires that a Licensed Product be compliant and that (i) does not include instructions or data other than such instructions or data that are permanently embedded in such device or component; or (ii) includes instructions or data that are not permanently embedded in such device or component where such instructions or data have been customized for such Licensed Product or Licensed Component and such instructions; or (iii) data are not accessible to the end user through the Licensed Product or Licensed Component. Such implementations shall:

(a) Comply with Section 1.3 of this Exhibit C by any reasonable method including but not limited to embedding Device Keys and Highly Confidential cryptographic algorithms in silicon circuitry or firmware that cannot reasonably be read, or employing the techniques described above for Software.

(b) Be designed such that attempts to remove, replace, or reprogram Hardware elements in a way that would compromise the content protection requirements of SmartRight (including compliance with the Compliance Rules and Specification) in Licensed Products would pose a serious risk of rendering the Licensed Product unable to receive, decrypt, or decode SmartRight Content. By way of example, a component that is soldered rather than socketed may be appropriate for this means.

3.5 **SmartRight Smart Cards.** SmartRight Smart Cards shall include all of the characteristics set forth in Sections 1 and W of this Exhibit C. In particular, and without limiting the generality of the foregoing, all Terminal Cards shall comply with an ISO/IEC 1540 terminal card protection profile set of criteria applicable to all SmartRight Smart Cards as defined in the Specification.

3.6 **Hybrid.** The interfaces between Hardware and Software portions of a Licensed Product shall be designed so that the Hardware portions comply with the level of protection that would be provided by a pure Hardware implementation, and the Software portions comply with the level of protection which would be provided by a pure Software implementation.

3.7 **Level of Protection.** "Core Functions" of SmartRight include encryption, decryption, authentication, the limitations on use, storage, recording and output set forth in the Compliance Rules, maintaining the confidentiality of Highly Confidential cryptographic algorithms and Keys and preventing unauthorized exposure of Protected Content. The Core Functions of SmartRight shall be implemented in a reasonable method so that they cannot be defeated or circumvented merely by using general-purpose tools or equipment that are widely available at a reasonable price, such as screwdrivers, jumpers, clips and soldering irons ("Widely Available Tools"), or using specialized electronic tools or specialized software tools that are widely available at a reasonable price, such as EEPROM readers and writers, debuggers or decompilers ("Specialized Tools"), other than devices or technologies whether Hardware or Software that are designed and made available for the specific purpose of bypassing or circumventing the protection technologies required by DTCP ("Circumvention Devices"); and only with difficulty be defeated or circumvented using professional tools or equipment, such as logic analyzers, chip disassembly systems, or in-circuit emulators or any other tools, equipment, methods, or other techniques such as would be used primarily by persons of professional skill and training, but not including professional tools or equipment that are made available only on the basis of a non-disclosure agreement or Circumvention Devices.

3.8 **Advance of Technology.** Although an implementation of a Licensed Product when designed and first shipped may meet the above standards, subsequent circumstances may arise which, had they existed at the time of design of a particular Licensed Product, would have caused such products to fail to comply with these Robustness Rules ("New Circumstances"). If an Adopter has (a) actual notice of New Circumstances, or (b) actual knowledge of New Circumstances (the occurrence of (a) or (b) hereinafter referred to as "Notice"), then within eighteen (18) months after Notice such Adopter shall cease distribution of such Licensed Product and shall only distribute Licensed Products that are compliant with the Robustness Rules in view of the then-current circumstances.

#### 4. EXAMINATION

4.1 **Generally.** If the Association so requests via the Authority, Adopter shall provide, once per model or version of product, any publicly available technical design documentation and, under a reasonable, mutually-acceptable non-disclosure agreement, the service manual for such product, in order to assist in the evaluation of the compliance of such product with these Robustness Rules.

4.2 **Inspection and Report.** Upon a reasonable and good faith belief that a particular hardware model or software version of a Licensed Product designed or manufactured by Adopter does not comply with the Robustness Rules then in effect for such Licensed Product, and upon reasonable notice to Adopter via the Authority, the Association may request Adopter to submit promptly to an independent expert (acceptable to Adopter, which acceptance shall not be unreasonably withheld) for inspection such detailed information as Adopter deems necessary to understand such product's implementation of the Specification and Compliance Rules, such as would be sufficient to determine whether such product complies with these Robustness Rules. Adopter's participation in this inspection procedure is voluntary; no adverse inference may be drawn from Adopter's refusal of the Association's request or refusal to participate, in whole or in part, in such inspection. The conduct of such inspection and the contents of any report made by the independent expert shall be subject to the provisions of a nondisclosure agreement, mutually-agreeable to the Association, Adopter, and such expert, such agreement not to be unreasonably withheld, that also provide protections for Confidential Information and Highly Confidential Information relating to SmartRight that are no less stringent than those provided for in this Agreement. Such examination and report shall be conducted at the sole expense of the Association. Nothing in this paragraph shall limit the role or testimony of such expert, if any, in a judicial proceeding under such protective orders as a court may impose. Adopter shall not be precluded or estopped from challenging the opinion of such expert in any forum; nor shall any party be entitled to argue that any greater weight or evidentiary presumption should be accorded to the expert report than to any other relevant evidence. This provision may not be invoked more than once per hardware model or software version, provided that such right of inspection shall include the right to re-inspect the implementation of such model or version if it has been revised in an effort to cure any alleged failure of compliance.

**EXHIBIT C-1**  
**ROBUSTNESS CHECKLIST**

**Notice:** This Checklist is intended as an aid to the correct implementation of the Robustness Rules for hardware and software implementations of the SmartRight Specification in a Licensed Product. The Authority strongly recommends that you complete this Checklist for each hardware model or software version of a Licensed Product before releasing any product and at a sufficiently early date in design, as well as during production, to avoid product compliance redesign delays. This Checklist does not address all aspects of the Specification and completion of this checklist is not sufficient to establish Compliance. Failure to perform necessary tests and analysis could result in a failure to comply fully with the Specification, Compliance Rules or Robustness Rules in breach of Adopter Agreement and, as a consequence, in appropriate legal action.

Notwithstanding whether any particular design or production work is being outsourced or handled by contractors to the company, compliance with the above Rules remains the responsibility of this company.

**DATE:** \_\_\_\_\_  
**MANUFACTURER:** \_\_\_\_\_  
**PRODUCT NAME:** \_\_\_\_\_

**HARDWARE MODEL OR SOFTWARE VERSION:** \_\_\_\_\_  
**NAME OF TEST ENGINEER COMPLETING CHECKLIST:**  
**TEST ENGI-**  
**NEER:** \_\_\_\_\_  
**COMPANY**  
**NAME:** \_\_\_\_\_

**COMPANY**

**ADDRESS:** \_\_\_\_\_

**PHONE**

**NUMBER:** \_\_\_\_\_

**FAX**

**NUMBER:** \_\_\_\_\_

**GENERAL IMPLEMENTATION QUESTIONS**

1. Has the Licensed Product been designed and manufactured so there are no switches, buttons, jumpers, or software equivalents of the foregoing, or specific traces that can be cut, by which the content protection technologies, analog protection systems, output restrictions, recording limitations, or other mandatory provisions of the Specification or Compliance Rules can be defeated or by which Protected Content can be exposed to unauthorized copying or use.?
2. Has the Licensed Product been designed and manufactured so there are no service menus and no functions (such as remote-control functions, switches, check boxes, or other means) that can intercept the flow of data or expose it to unauthorized copying?
3. Has the Licensed Product been designed and manufactured so there are no service menus and no functions (such as remote-control functions, switches, check boxes, or other means) that can turn off any analog protection systems, output restrictions, recording limitations, or other mandatory provisions of the Specification or Compliance Rules?
4. Does the Licensed Product have service menus, service functions, or service utilities that can alter or expose the flow of data within the device?

If Yes, please describe these service menus, service functions, or service utilities and the steps that are being taken to ensure that these service tools will not be used to expose or misdirect Decrypted SmartRight Content.

5. Does the Licensed Product have service menus, service functions, or service utilities that can turn off any analog protection systems, output restrictions, recording limitations,

or other mandatory provisions of the Specification or Compliance Rules?

If Yes, please describe these service menus, service functions, or service utilities and the steps that are being taken to ensure that these service tools will not be used to defeat the content protection features of SmartRight (including compliance with the Compliance Rules and the Specification).

6. Does the Licensed Product have any User Accessible Buses (as defined in Section 1.52 of the Robustness Rules)?

If so, is Protected Content carried on this bus?

If so, then: identify and describe the bus, and whether the Protected Content is compressed or uncompressed. If such Data is compressed, then explain in detail how and by what means the data is being protected as required by Section 2.2 of the Compliance Rules.

7. Explain in detail how the Licensed Product protects the confidentiality of all Keys.

8. Explain in detail how the Licensed Product protects the confidentiality of the confidential cryptographic algorithms used in SmartRight.

9. If the Licensed Product Protected Content from one part of the product to another, whether among software modules, integrated circuits or otherwise or a combination thereof, explain how the portions of the product that perform authentication and decryption and the MPEG (or similar) decoder have been designed, associated and integrated with each other so that Protected Content is secure from interception and copying as required in Section 3.1 of the Robustness Rules.

10. Are any SmartRight functions implemented in Hardware?

If Yes, complete hardware implementation questions.

11. Are any SmartRight functions implemented in Software?

If Yes, complete software implementation questions.

## **SOFTWARE IMPLEMENTATION QUESTIONS**

12. In the Licensed Product, describe the method by which all Keys are stored in a protected manner.

13. Using the grep utility or equivalent, are you unable to discover any Keys in binary images of any persistent memory devices?

14. In the Licensed Product, describe the method used to obfuscate the confidential cryptographic algorithms and Keys used in SmartRight and implemented in software.

15. Describe the method in the Licensed Product by which the intermediate cryptographic values (e.g., values created during the process of authentication between modules or devices within a Licensed Product) are created and held in a protected manner.

16. Describe the method being used to prevent commonly available debugging or de-

compiling tools (e.g., Softice) from being used to single-step, decompile, or examine the operation of the SmartRight functions implemented in software.

17. Describe the method by which the Licensed Product self-checks the integrity of component parts in such manner that modifications will cause failure of authorization or decryption as described in Section 3.2.2 of the Robustness Rules. Describe what happens when integrity is violated.

18. To assure that integrity self-checking is being performed, perform a test to assure that the executable will fail to work once a binary editor is used to modify a random byte of the executable image containing SmartRight functions, and describe the method and results of the test.

## **HARDWARE IMPLEMENTATION QUESTIONS**

19. In the Licensed Product, describe the method by which all Keys are stored in a protected manner and how their confidentiality is maintained.

20. Using the grep utility or equivalent, are you unable to discover any Keys in binary images of any persistent memory devices?

21. In the Licensed Product, describe how the confidential cryptographic algorithms and Keys used in SmartRight have been implemented in silicon circuitry or firmware so that they cannot be read.

22. Describe the method in the Licensed Product by which the intermediate cryptographic values (e.g., values created during the process of authentication between modules or devices within a Licensed Product) are created and held in a protected manner.

23. Describe the means used to prevent attempts to replace, remove, or alter hardware elements or modules used to implement SmartRight functions.

24. In the Licensed Product, does the removal or replacement of hardware elements or modules that would compromise the content protection features of SmartRight (including the Compliance Rules, the Specification, and the Robustness Rules) damage the Licensed Product so as to render the Licensed Product unable to receive, decrypt, or decode SmartRight Content?

**Notice: This checklist does not supersede or supplant the SmartRight Specification, Compliance Rules, or Robustness Rules. The Company and its Test Engineer are advised that there are elements of the Specification and Compliance Rules that are not reflected here but that must be complied with.**



**SIGNATURES:**

Signature of Test Engineer with Personal Knowledge of Answers

Date

Printed Name of Test Engineer with Personal Knowledge of Answers

**APPENDIX B**  
**SMARTRIGHT CONTENT PARTICIPANT AGREEMENT**  
**(APRIL 16, 2004)**



## CONTENT PARTICIPANT AGREEMENT

This SmartRight Content Participant Agreement (the “Agreement”) is effective as of the latest date set out on the signature page hereof (the “Effective Date”) by and between the SmartRight Licensing Authority, LLC (the “Authority”) and the entity named on the signature page (together with its Affiliates, “Content Participant”).

### RECITALS

WHEREAS, the Authority is the authorized licensor of the SmartRight® system for protecting certain digital content from unauthorized use as described in the SmartRight Specification (the “Specification”);

WHEREAS, Content Participant wishes to have the right, subject to the terms and conditions set forth herein, to use such technology to protect its audiovisual works and to obtain certain other rights, including but not limited to certain rights to seek Revocation and Renewal (as such terms are defined below);

NOW, THEREFORE, in consideration of the foregoing and the covenants and agreements set forth herein, the parties hereto hereby agree as follows:

### TERMS OF AGREEMENT

1. **DEFINITIONS.** In addition to terms defined elsewhere in this Agreement, the following terms shall have the following meanings:

1.1 “Administration Fee” has the meaning set forth in Section 4.1.

1.2 “Adopter” means any entity that has executed an Adopter Agreement with Authority and delivered it to Authority or its designee, and shall include any Affiliate of such entity.

1.3 “Adopter Agreement” means any “SmartRight Adopter Agreement” entered into by Authority and any Adopter of SmartRight, substantially in the form of Exhibit B hereto.

1.4 “Affected Adopter” means, with respect to a Device for which Revocation is requested or contemplated, any Adopter to whom Authority or Key Generator has issued the Device Key under such Adopter’s Adopter Agreement.

1.5 “Affiliate” means (unless specifically agreed otherwise in writing by Authority and such Person), with respect to any Person, any other Person directly or indirectly controlling or controlled by or under direct or indirect common control with such Person. “Control” means the possession of beneficial ownership of more than 50% of the stock or other similar interest entitled to vote for election of the Board of Directors or similar managing authority.

1.6 “Arbitrating Content Participant” has the meaning set forth in Section 3.6.4.

1.7 “Arbitrating Parties” has the meaning set forth in Section 3.6.4(v).

1.8 “Association” means the SmartRight Association, Inc., a not for profit corporation established to administer the Renewal or Revocation of SmartRight Products on behalf of Fellow Content Participants, Adopters and the Authority in conformity with the Procedural Rules. Membership in the Association is open to Content Participant and all Fellow Content Participants that choose to join the Association.

1.9 “Audiovisual Content” means audiovisual works (as defined in 17 U.S.C. § 101. .

1.10 “Authority” has the meaning set forth in the preamble to this Agreement.

1.11 “Compliance Rules” means the requirements set out in the exhibit entitled “Compliance Rules” to each Adopter Agreement, as such exhibits may be revised by Authority from time to time in accordance with Section 3.6 hereof.

1.12 “Conditional Access Content” has the meaning set forth in the Compliance Rules.

1.13 “Confidential Information” means all information disclosed by either party to this Agreement that has been identified or designated to be confidential and proprietary, or that a reasonable person would judge to be confidential under the circumstances, including without limitation, any information concerning unpublished copyrighted works or mask works, unpublished pending patent applications, development materials, source code, unmarketed products or components, design documentation, system documentation specifications, and any information regarding such party’s financial, business, and marketing matters. Except as provided in Section 6.3.2, Confidential Information

includes Highly Confidential Information. A party's status as an Adopter, or lack thereof, shall not be deemed Confidential Information.

1.14 "Content Participant" has the meaning set forth in the preamble to this Agreement.

1.15 "Content Participant Agreement" means this Agreement and any other "SmartRight Content Participant Agreement" entered into by Authority and a provider of Audiovisual Content.

1.16 "Content Participant Beneficiaries" has the meaning set forth in Section 3.3.

1.17 "Content Participant Beneficiary Claim" has the meaning set forth in Section 3.3.

1.18 "Content Participant Contact" has the meaning set forth in Section 6.5.

1.19 "Contract Year" means any one (1) year period beginning on the Effective Date or any anniversary thereof.

1.20 "CP Affidavit" has the meaning set forth in Section 5.3.1.

1.21 "Decrypted SmartRight Content" has the meaning set forth in the Compliance Rules.

1.22 "Device Key" means a cryptographic value provided to an Adopter by Authority or its designee for use in a Licensed Product.

1.23 "Disclosing Party" has the meaning set forth in Section 6.1.

1.24 "Effective Adopter Agreements" has the meaning set forth in Section 3.5.2.

1.25 "Effective Date" has the meaning set forth in the preamble to this Agreement.

1.26 "Eligible Content Participant" means any Content Participant that is in compliance with all of the material terms and conditions of its Content Participant Agreement.

1.27 "Fellow Content Participant" means any provider of Audiovisual Content, including Content Participant, that has entered into a Content Participant Agreement.

1.28 "Form Adopter Agreement" means the form Adopter Agreement attached hereto as Exhibit B.

1.29 "Highly Confidential Information" means Confidential Information of the Authority that is marked "Highly Confidential Information" or otherwise designated as such by the Authority. All Device Keys are Highly Confidential Information.

1.30 "Key Generator" means the generator of Device Keys designated by Authority.

- 1.31 “Licensed Component” means a product, such as an integrated circuit, circuit board, or software module, that is designed to be incorporated into a Licensed Product and that embodies any SmartRight Technology.
- 1.32 “Licensed Patents” means all Necessary Claims of the patents and applications which the Authority has been authorized to license.
- 1.33 “Licensed Product” means a Finished License Product or a Licensed Component.
- 1.34 “Licensed Technology” means the Licensed Patents, the Specification and all trade secrets, copyrights, mask rights and other exclusive rights which relate thereto.
- 1.35 “Major Content Participant” means, during the course of any year, any Fellow Content Participant that either is a member of the Motion Picture Association of America or has generated U.S. box office revenues from theatrical releases of feature films in the immediately prior year that are at least as great as the MPAA member company with the lowest U.S. box office revenues from theatrical releases of feature films for that same year.
- 1.36 “Necessary Claims” means claims of a patent or patent application that would be necessarily and unavoidably infringed by the manufacture, use, sale, offer for sale or import or other disposition of a product or by the practice of any method required in order to comply with the SmartRight Specification in a particular country in the absence of a license or other authorization from the owner of such patent claims in such country. As used herein, “infringe” includes direct infringement, contributory infringement and/or inducement of infringement. Essential Patent Claims shall not include patent claims for a technology that has been developed by third parties independent of the SmartRight System but has been incorporated and referenced in the Specification for use in the SmartRight System.
- 1.37 “Operative Protection Agreements” has the meaning set forth in Section 3.5.2.
- 1.38 “Party” means a party to this Agreement.
- 1.39 “Person” means any natural person, corporation, partnership, or other entity.
- 1.40 “Presentation Device” has the meaning set forth in the Compliance Rules.
- 1.41 “Receiving Party” has the meaning set forth in Section 6.1.
- 1.42 “Renewal” has the meaning set forth in Section 5.1.
- 1.43 “Renewal Criteria” means those criteria for Renewal set forth in Section 5.3.3.
- 1.44 “Revocation” or “Revoked” has the meaning set forth in the definition of Revoke.
- 1.45 “Revocation Arbitration” means the arbitration procedure initiated pursuant to Section 5.3.1.

1.46 “Revocation Information” means information distributed to Fellow Content Participants by or under the direction of Authority for purposes of distributing such information with Audiovisual Content in order to Revoke, or rescind the Revocation of, one or more Keys.

1.47 “Revoke” means, with respect to a Key Selection Vector, to distribute information, as authorized or provided by Authority, to Fellow Content Participants for purposes of their distributing such information with Audiovisual Content in order to cause a Device Keys or Session Keys to be invalidated with respect to such content (generally, “Revocation” or “Revoked”).

1.48 “Robustness Rules” means the requirements set out in the exhibit entitled “Robustness Rules” to each Adopter Agreement, as such exhibit may be revised by Authority from time to time in accordance with Section 3.6 hereof.

1.49 “SmartRight” means the SmartRight system for protecting certain digital content from unauthorized use as described in the Specification.

1.50 “SmartRight Content” means content that has been encrypted and packaged with a Local Enforcement Copy-Management Message (“LECM”) in accordance with the SmartRight Specification. SmartRight Content includes Encrypted SmartRight Content and Decrypted SmartRight Content. For avoidance of doubt, “SmartRight Content” does not include content that has never been encrypted by SmartRight.

1.51 “SmartRight Participants” means the Authority, all Adopters, all Fellow Content Participants and their Affiliates.

1.52 “SmartRight Proposed Action” has the meaning set forth in Section 3.6.1.

1.53 “Specification” means the document entitled “SmartRight Specification” issued by the Authority, as may be amended from time to time pursuant to Section 3.3 of the Adopter Agreement, and Section 3.6 of the Content Participant Agreement.

1.54 “System Renewability Message” has the meaning given in the SmartRight Specification.

1.55 “Third Party Beneficiary Claim” has the meaning set forth in Section 1.1.

## 2. LICENSES.

2.1 License to Use SmartRight. Subject to the terms and conditions of this Agreement, including but not limited to Content Participant’s material compliance with Section 2.2 and payment of fees required hereunder, Authority hereby grants to Content Participant a nonexclusive, nontransferable (except pursuant to Section 12.3), non-sublicenseable, worldwide license under the Licensed Technology to use, and to cause or permit SmartRight to be used, to protect Conditional Access Content in connection with the distribution and transmission of such Conditional Access Content.

2.2 Reciprocal Licensing Agreement. In the event Adopter, now or in the future, owns or controls any Necessary Claims, and subject to the limitations set forth in Section 2.3, Content Participant, on behalf of itself and its Affiliates, shall either (a) not assert or maintain such claims against any SmartRight Participants for making, having made, using, importing, offering to sell or selling Licensed Products, or for engaging in any activities for which any of those persons have been granted a license by the Authority; or (b) offer to license all SmartRight Participants under any Necessary Claims owned or controlled by Content Participant or its Affiliates, on terms that are fair, reasonable and non-discriminatory, the right to make, have made, use, import, offering to sell and sell Licensed Products.

2.3 Limitations on Sections 2.1 and 2.2. The license and promises set out in Sections 2.1 and 2.2 shall not extend to (a) features of a product that are not required to comply with, or aspects of any technology, codec, standard or product not disclosed with particularity in, the SmartRight Specification, even if such technology, codec, standard, or product may be mentioned in the SmartRight Specification, Compliance Rules or Robustness Rules; (b) features of a product for which there exists a noninfringing alternative; (c) any Fellow Content Participant who is in breach of its obligations under its Content Participant Agreement; or (d) activities or products performed or made after a Person has ceased to be a Content Participant.

2.4 Liability for Affiliates. Content Participant shall procure and be responsible for its Affiliates' compliance with the terms and conditions of this Agreement, and such entity and each of its Affiliates shall be jointly and severally liable for any noncompliance by any such Affiliate with the terms and conditions of this Agreement.

### 3. **ADDITIONAL RIGHTS GRANTED TO CONTENT PARTICIPANT.**

3.1 Content Participant shall have the right to associate membership in the Association. In the event that Content Participant elects to become an associate member of the Association, it shall so notify the Authority upon such election. Content Participant may, by notice to the Authority, change its status as an associate member or non-associate member of the Association. Upon request of the Association, or a majority of the associate member companies of the MPAA that are Content Participants, the Authority shall undertake to take into account the views expressed by the Association with respect to (a) the Compliance Rules as of the Effective Date; (b) any future technical or other amendments thereto (such as with respect to extending SmartRight to additional technologies); and (c) such other matters relating to SmartRight as the Authority and the associate members of the Association may agree to discuss.

3.2 Right to Seek Revocation. For so long as Content Participant is an Eligible Content Participant, it shall have the right to seek Revocation or Renewal pursuant to the terms of Article 5.

3.3 Content Participant Third-Party-Beneficiary Rights. For so long as Content Participant is an Eligible Content Participant, it shall be a third-party beneficiary of each Adopter Agreement (Content Participant, together with any one or more other Eligible



Fellow Content Participants, “Content Participant Beneficiaries”), and, as such, shall be entitled to bring a claim or action to enforce such third-party-beneficiary rights against an Adopter as are specified in such Adopter’s Adopter Agreement (such claim or action, together with any third-party-beneficiary claim brought by any other Content Participant Beneficiary, a “Content Participant Beneficiary Claim”), and to have such remedies as are set forth in such Adopter Agreement in accordance with the procedures set forth in this Article 3. Exercise of its third-party-beneficiary rights under any Adopter Agreement shall not constitute an election against any statutory or other extra-contractual remedy against an Adopter which may be available to Content Participant for the same act which gave rise to the Content Participant Beneficiary Claim.

3.4 Enforcement Actions. For so long as Content Participant is an Eligible Content Participant: (a) it shall have the right to communicate with Authority with respect to the status of enforcement actions that are brought by Authority to enforce an Adopter’s compliance with its Adopter Agreement and that may reasonably implicate Content Participant’s Audiovisual Content, and (b) Authority shall respond to inquiries from Content Participant with respect to such enforcement actions, subject to any confidentiality obligations that may apply under any Adopter Agreement.

3.5 Change Management.

3.5.1 Effective Documents. Authority represents that, as of the Effective Date, the following documents are the only documents establishing the rights and obligations of Adopters with respect to SmartRight:

- Adopter Agreements, including their attachments and documents incorporated therein by reference;
- The Specification;
- Other interpretive and clarifying documents relating to the licensing of SmartRight posted on the website of Authority as of the Effective Date, including by way of example and not limitation, policy statements of Authority, side-letters with certain Adopters, and clarifications of the Adopter Agreements;
- Non-Disclosure Agreements; and
- Content Participant Agreements.

Authority further represents that, as of the Effective Date, all Adopter Agreements entered into after the Effective Date shall be substantially in the form of the Adopter Agreement attached hereto as Exhibit B (“Form Adopter Agreement”); provided, however, that such Form Adopter Agreement may be amended from time to time in accordance with Section 3.6. “Substantially in the form” means that only variations from the Form Adopter Agreement which (i) are authorized pursuant to Section 3.6, or (ii) are not required to be subject to notice under

Section 3.6.1, are permitted. Authority will make all Adopter Agreements entered into available to Content Participant on request.

3.5.2 Consistency with Form Adopter Agreement. Authority represents that, as of the Effective Date, except as otherwise disclosed in writing to Content Participant: (a) the Adopter Agreements in effect as of the Effective Date (the “Effective Adopter Agreements”), together with all other documents described in Section 3.5.1 in effect as of the Effective Date (collectively, the “Operative Protection Agreements”), are consistent in all material respects affecting the integrity or security of SmartRight, or the operation of SmartRight with respect to protecting Audiovisual Content from any unauthorized output, transmission, interception or copying, or the rights of Content Participant with respect to SmartRight, with the Form Adopter Agreement; and (b) there are no oral or written amendments or understandings with any Adopter varying or modifying such Effective Adopter Agreements or other Operative Protection Agreements, other than as specifically set forth in the Operative Protection Agreements with respect to such integrity, security, operation, or the rights of Content Participants. Content Participant may review the Operative Protection Agreements upon reasonable notice to Authority.

### 3.6 Changes In Protection of Rights.

3.6.1 Authority shall provide reasonable advance written notice to Content Participant and identify with specificity: (1) any proposed change, addition or supplement to Articles I (Definitions), III (Specification and Compliance Rules), IV (Revocation and Renewal), V (License), VI (Distribution and Qualification of Products), VII (Confidentiality), VIII (Term/Termination), X (Remedies) and XI (Miscellaneous) of any Effective Adopter Agreement (including equivalent sections that may be numbered or titled differently), of the Form Adopter Agreement or of any copy of the Form Adopter Agreement entered into by an Adopter after the date of this Agreement, and to the Compliance Rules of any Effective Adopter Agreement or of the Form Adopter Agreement; (2) any proposed change, addition, or supplement to any other Operative Protection Agreements (other than the Specification) that would affect the integrity or security of SmartRight, or the operation of SmartRight with respect to protecting Audiovisual Content from any unauthorized output, transmission, interception or copying, or the rights of Content Participant with respect to SmartRight; (3) the proposed issuance, execution or amendment by Authority of any other document that would affect the integrity or security of SmartRight, or the operation of SmartRight with respect to protecting Audiovisual Content from any unauthorized output, transmission, interception or copying, or the rights of Content Participant with respect to SmartRight; and (4) any proposed change, addition, or supplement to the Specification affecting Audiovisual Content, provided, however, that (x) Authority’s advance written notice with respect to any such change to the Specification shall be sent to Content Participant only if Content Participant has executed and delivered to Authority a non-disclosure agreement satisfactory to Authority and (y) Authority shall, during the second calendar quarter of each year,

make available to Content Participant any changes to the Form Adopter Agreement not otherwise noticed pursuant to Section 3.6; provided further, that if Content Participant objects to any of such changes described in (y), Authority will disclose to Content Participant, upon request, any similar changes that were made to Adopter Agreements and (z) changes to the Specification that may be necessary to map the Specification to support auxiliary data extensions shall not be regarded as “material” or “adverse” for purposes of, or otherwise subject to, this Section 3.6. For purposes of this Agreement, each of the items as to which Content Participant is to receive advance written notice as described in clauses (1) to (4), hereof, inclusive, is a “SmartRight Proposed Action.”

3.6.2 Except as otherwise expressly provided in this Section 3.6, for so long as Content Participant is an Eligible Content Participant, it shall have the right, either on its own or with one or more Fellow Content Participants that are each an Eligible Content Participant under its Content Participant Agreement, to file a written objection to any SmartRight Proposed Action that it believes would have a material and adverse effect on the integrity or security of SmartRight, or the operation of SmartRight with respect to protecting Audiovisual Content from any unauthorized output, transmission, interception or copying, or the rights of Content Participant with respect to SmartRight. Any such objection shall set forth with specificity the alleged material and adverse effects on the integrity or security of SmartRight, or the operation of SmartRight (including the protections provided by the Compliance Rules and Robustness Rules) with respect to protecting Audiovisual Content from any unauthorized output, transmission, interception or copying, or the rights of Content Participant with respect to SmartRight, and shall be delivered to Authority no later than thirty (30) business days after the date of service of notice by Authority pursuant to Section 3.6.1 at the address specified in the notice provisions of this Agreement. In the event Authority has served such notice to Content Participant by (x) mail postmarked in the same country as the country in which Content Participant is to receive notices, three (3) days shall be added to the prescribed period for filing an objection, (y) mail postmarked in a country other than the country in which Content Participant is to receive notices, fifteen (15) days shall be added to the prescribed period for filing an objection.

3.6.3 Authority agrees to consider any such objection given pursuant to Section 3.6.2 in good faith. If Authority rejects such objection, it shall provide prompt written notice thereof to Content Participant and any Fellow Content Participants that filed a written objection explaining, with specificity, the reasons for such rejection and why the action would not be material or have an adverse effect, including the benefits that would be afforded by the SmartRight Proposed Action. Absent delivery to Authority of written objection from one or more Fellow Content Participants pursuant to Section 3.6.2, Authority may take the applicable SmartRight Proposed Action.

3.6.4 If (x) Content Participant is a Major Content Participant and has objected to a SmartRight Proposed Action pursuant to Section 3.6.2, (y) Content

Participant is joined by other Fellow Content Participants that are Major Content Participants and also are Eligible Content Participants under each of their Content Participant Agreements, which, together with Content Participant, constitute a majority of Major Content Participants that are also Eligible Content Participants, and (z) such majority continues to object to the SmartRight Proposed Action notwithstanding communication with Authority pursuant to Section 3.6, then Content Participant and such Fellow Content Participants shall have the right, within thirty (30) days from receipt of Authority's rejection of such objection pursuant to Section 3.6.2 to initiate an arbitration in accordance with the provisions of this Section 3.6.4:

(i) The Authority, interested Content Participants, and the Adopters shall attempt in good faith to resolve the objections to the proposed change during the sixty (60) day period following the delivery of the notice of the objections.

(ii) At any time during such sixty day period, any Eligible Content Participants who have filed timely objections (the "Arbitrating Content Participants") may request arbitration to resolve the dispute by sending to the Authority a notice of intention to arbitrate in accordance with the commercial arbitration rules of the American Arbitration Association (the "Rules"). The parties shall thereafter proceed to arbitrate the dispute in accordance with this Section 3.6.4.

(iii) In such arbitration, the Arbitrating Content Participants shall have the burden of demonstrating, based on the preponderance of evidence, that the SmartRight Proposed Action is material and adversely affects the integrity or security of SmartRight, or the operation of SmartRight (including the protections provided by the Compliance Rules and Robustness Rules) with respect to protecting Audiovisual Content from any unauthorized output, transmission, interception or copying, or the rights of the Arbitrating Content Participants with respect to SmartRight (for purposes of this Section 3.6, "material and adverse"). Changes that only insignificantly diminish the integrity, security or operation of SmartRight with respect to protecting Audiovisual Content from any unauthorized output, transmission, interception or copying, or the rights of Content Participants with respect to SmartRight, shall not be deemed "material" or "adverse." Notwithstanding the above, the arbitrator(s) may, in his, her or their discretion take into consideration the cumulative effect of multiple related changes made within the then-preceding two (2) year period that are not material and adverse when considered in isolation, provided that in any such consideration the arbitrator(s) afford(s) countervailing weight to any changes made within the then-preceding two (2) year period, whether related or not, that have had or, when implemented, will have a beneficial effect on the integrity or security of SmartRight or the operation of SmartRight with respect to protecting Audiovisual Content from any unauthorized output, transmission,

interception or copying, or the rights of Content Participants with respect to SmartRight.

(iv) Where the Arbitrating Content Participants have the burden of demonstrating that the SmartRight Proposed Action is material and adverse, if they have carried such burden, then Authority may not take the SmartRight Proposed Action unless Authority demonstrates, based on the preponderance of evidence, that the SmartRight Proposed Action provides a material legal benefit in the form of avoidance of a reasonably-perceived potential legal liability to Authority or Adopters which cannot practicably be achieved except by taking the SmartRight Proposed Action.

(v) There shall be a sole arbitrator, who shall be selected by Authority and the Arbitrating Content Participants (collectively, the “Arbitrating Parties”) from the National Panel of Commercial Arbitrators of the American Arbitration Association within fourteen (14) days of the initiation of arbitration, provided, however, that in the event the Arbitrating Parties cannot agree on a sole arbitrator within such fourteen (14) day period, Authority, on the one hand, and the Arbitrating Content Participants, on the other, shall each, promptly thereafter, select one arbitrator from the National Panel of Commercial Arbitrators of the American Arbitration Association and those two (2) arbitrators shall jointly select a third arbitrator from the National Panel of Commercial Arbitrators of the American Arbitration Association, who shall serve as the presiding arbitrator and chairperson of such arbitration.

(vi) The Arbitrating Content Participants, on the one hand, and Authority, on the other, shall, during the course of the arbitration, share equally the costs of arbitration set forth in this Section 3.6(e), provided, however, that the arbitrator(s) shall award the prevailing party or parties all of its or their costs and expenses, other than attorneys’ fees and expenses. In addition, if the arbitrator(s) find(s) that either Authority or the Arbitrating Content Participants has or have advanced its or their position in bad faith or frivolously, it (they) shall order such party or parties to reimburse the other party or parties for its or their reasonable attorneys’ fees and expenses.

(vii) The arbitrator(s) is (are) empowered solely to determine (1) whether the Arbitrating Content Participants have carried their burden of demonstrating that a SmartRight Proposed Action is material and adverse and (2) whether or not based solely upon the standards in Section 3.6.4(iii) and Section 3.6.4(iv), the Authority may take a particular SmartRight Proposed Action.

(viii) The arbitration specified in this Section 3.6.4 shall be conducted in accordance with the following provisions:

(a) The arbitration shall be conducted in Los Angeles, California, in accordance with the International Arbitration Rules of the American Arbitration Association. The language of the arbitration shall be English.

(b) The arbitrator(s) may conduct the arbitration in such manner as he, she or they shall deem appropriate, including the imposition of time limits that he, she or they consider(s) reasonable for each phase of the proceeding, but with due regard for the need to act, and make a final determination, in an expeditious manner. The arbitrator(s) shall set a schedule to endeavor to complete the arbitration within one (1) month.

(c) The arbitrator(s) shall permit and facilitate such limited discovery as he, she or they shall determine is reasonably necessary, taking into account the needs of the Arbitrating Parties and the desirability of making discovery as expeditious and cost-effective as possible, recognizing the need to discover relevant information and that only one party may have such information.

(d) The Arbitrating Parties and the arbitrator(s) shall treat the arbitration proceedings, any related discovery, documents and other evidence submitted to, and the decision of, the arbitrator(s) as Confidential Information. In addition, and as necessary, the arbitrator(s) may issue orders to protect the confidentiality of proprietary information, trade secrets and other sensitive information disclosed in discovery or otherwise during the arbitration.

(e) Any decision by the arbitrator(s) shall be final and binding on the Arbitrating Parties, except that whether the arbitrator(s) exceeded his, her or their authority, as specifically described in this Agreement, shall be fully reviewable by a court of competent jurisdiction. Judgment upon any award shall be entered in a court of competent jurisdiction.

(f) The arbitrator(s) shall be compensated at his, her or their hourly rates, determined at the time of appointment, for all time spent in connection with the arbitration, and shall be reimbursed for reasonable travel and other expenses. The arbitrator(s) shall determine all costs of the arbitration, including the arbitrator(s)' fees and expenses, the costs of expert advice and other assistance engaged by the arbitrator(s), the cost of a transcript and the costs of meeting and hearing facilities.

3.6.5 If (i) no arbitration has been initiated with respect to the SmartRight Proposed Action pursuant to Section 3.6.4 or (ii) the arbitrator(s) determine(s)

that the Arbitrating Content Participants have not carried their burden of demonstrating that the SmartRight Proposed Action is material and adverse, then Authority may take the SmartRight Proposed Action, and such action may be effective, according to its terms, thirty (30) days after receipt of Authority's rejection pursuant to Section 3.6.3 or such final determination of the arbitrator(s). In the event that the inability to take the SmartRight Proposed Action exposes Authority to potential legal liabilities based on a claim of infringement which cannot practically be avoided except by taking the SmartRight Proposed Action, and the Arbitrating Content Participants nonetheless continue to object to the SmartRight Proposed Action, Authority and the Arbitrating Content Participants shall discuss in good faith whether and in what circumstances Authority can continue to license SmartRight, taking into account considerations, including but not limited to (x) Arbitrating Content Participants' and other content owners' willingness and ability to indemnify all SmartRight Participants with respect to such claim, (y) other costs and liabilities to SmartRight Participants, and (z) possible conversion of any licenses relating to SmartRight to covenants not to assert intellectual property claims. If, after such discussions, the Arbitrating Content Participants and Authority are unable to agree on the circumstances in which Authority would be willing to continue to license SmartRight, Authority may terminate this Agreement and any other adopter agreement relating to SmartRight.

4. **ADMINISTRATION FEES.**

4.1 Administration Fee. Within thirty (30) days of the Effective Date and of each anniversary of the Effective Date, Content Participant shall pay Authority the amount set out in Exhibit A (as such amount may be adjusted in accordance with this Section 4.1, the "Administration Fee"). As of the first anniversary of the Effective Date, and on an annual basis thereafter, Authority shall have the right, upon at least thirty (30) days' notice to Content Participant, to adjust the Administration Fee on a reasonable and nondiscriminatory basis, provided that any increase in such fee shall not exceed an amount commensurate with any increase in Authority's costs (including, but not limited to, the cost of inflation). Content Participant shall not be entitled to any refund of Administration Fees for any reason except as expressly provided in Section 8.1.2.

5. **REVOCATION; RENEWAL.**

5.1 Generally. The Specification includes means by which Keys may be invalidated (generally, "Revocation" or "Revoke"). In addition, SmartRight Smart Cards and all attributes of SmartRight Products capable of being modified by a Smart Card may also be replaced or modified through the distribution of new SmartRight Smart Cards (generally, "Renewal" or "Renew"). The "Association" shall have the right to determine whether any Keys may be Revoked or SmartRight Products Renewed in accordance with this Article 5.

5.2 Obligation to Carry Revocation Information. The Association shall notify Content Participant in the event that Association plans to Revoke or rescind the

Revocation of any Keys, or Renew all or part of the SmartRight System, and shall deliver or cause to be delivered to Content Participant Revocation Information for use in connection with such Revocation, rescission of Revocation or Renewal. In the case of any Revocation, rescission of Revocation or Renewal, Content Participant shall use commercially reasonable efforts to include or cause the inclusion of the latest Revocation Information provided by the Association. In no case shall Content Participant be required to, or cause on its behalf to, (a) remaster any of Content Participant's Audiovisual Content, or (b) include or cause the inclusion of Revocation Information in previously manufactured copies of Content Participant's Audiovisual Content.

### 5.3 Content Participant Request for Revocation or Renewal.

5.3.1 For so long as Content Participant is an Eligible Content Participant, it shall have the right, either on its own or with one or more Fellow Content Participants who is (are) each an Eligible Fellow Content Participant(s) under its (their) respective Content Participant Agreement(s), to seek Revocation or Renewal by providing to the Association proof in a sworn affidavit (the "CP Affidavit") of any of the facts relating to the need for revocation or renewal that would satisfy the Revocation Criteria or Renewal Criteria (defined below); provided, however, that such CP Affidavit shall be sufficiently detailed such that Authority can determine solely on the basis of such affidavit whether the facts averred satisfy one or more of the Revocation Criteria or Renewal Criteria. For so long as Content Participant is an Eligible Content Participant, the Association shall initiate the Revocation procedures set forth in Section 5.3.4 if the affidavit satisfies the requirements of this Section 5.3.1. However, the Association shall have sole discretion to determine whether to act upon a request for Renewal.

5.3.2 Revocation Criteria. In the event that Content Participant or any other Fellow Content Participant seeks Revocation of a Key or Keys, at least one of the following criteria (the "Revocation Criteria") must be satisfied:

- (a) A Device Key has been copied such that the same Key is found in more than one device or product;
- (b) A Key has been lost, stolen, intercepted or otherwise misdirected, or made public or disclosed;
- (c) A Network Key is present in more Terminal Modules than permitted by the Maximum Network Size; or
- (d) The Association is required to revoke a Key by court order, or other competent government Authority.

5.3.3 Renewal Criteria. In the event that Content Participant or any other Fellow Content Participant seeks Renewal of all or Part of the SmartRight System, at least one of the following criteria (the "Renewal Criteria") must be satisfied:



- (a) The Association determines that unauthorized use or distribution of SmartRight content have reached a sufficient level to justify the cost of Renewal, or
- (b) The Association determines that it is feasible and desirable to upgrade the reliability and security of the SmartRight Technology; or
- (c) The Association is required to implement a change in outstanding SmartRight Smart Cards by court order, or other competent government Authority.

#### 5.3.4 Revocation Procedures.

- (a) Request for Revocation. If the owner of the SmartRight Product containing the Key sought to be revoked has provided an Adopter with information sufficient to permit communications to be addressed to such person (the "Registered Owner"), the Association, upon its own initiative, or at the request of a Fellow Content Participant, may request a Revocation of a Key or Keys by notifying the Registered Owner of the grounds upon which such Revocation is sought.
- (b) Revocation by Consent. If (i) the owner of the SmartRight Product containing the key sought to be Revoked has not provided information sufficient to permit communications to be addressed to such owner, (ii) Revocation is requested by the Registered Owner, or (iii) such Registered Owner consents to a request by the Association, the Association shall Revoke the Keys which are the subject of the request without further proceedings.
- (c) Procedure for Contested Revocation. Within thirty (30) days following issuance by the Association of a Request for Revocation, the Registered Owner of any SmartRight Product which is the subject of the Request may notify the Association of any objections to the request and the grounds therefor. Upon receipt of such objection, the Association shall take such measures as it deems appropriate to investigate and ascertain (a) whether grounds exist for Revocation and (b) whether such grounds constitute a sufficient threat to the integrity of the SmartRight System to justify the Revocation. If the Revocation was requested by an Eligible Content Participant, then such Content Participant will be consulted and permitted to participate in the investigation.

5.3.5 Judicial Review. The determination to Revoke or Renew a Key or Renew any SmartRight Products shall be made solely in the discretion of the Association giving due regard to the interests of content owners, content distributors, adapters and device owners whose interests may be affected thereby, and shall be subject to review in accordance with the procedures set forth in Article 78 of the New York Civil Practice Law and Rules upon the grounds set forth in Section 7803, subdivision 3 thereof.

5.3.6 Renewal Procedures. Upon its own initiative or upon the request of any third party whose rights have been adversely affected, the Association may

implement a procedure for Renewal of one or more SmartRight Products by notifying all SmartRight Participants having an interest in such products of its intention to seek such Renewal and the grounds upon which Renewal is sought.

(a) Within thirty (30) days following issuance by the Association of a Request for Renewal, any SmartRight Participants may make a submission to the Associations setting forth its views as to (i) whether grounds exist for Renewal, (ii) whether such grounds constitute a sufficient threat to the integrity of the SmartRight System to justify the Renewal and (iii) the appropriate allocation among the SmartRight Participants of the costs of implementing the Renewal and the manner in which such costs may be funded.

(b) Following the receipt of the submissions, the Association shall take such measures as it deems appropriate to investigate and to determine whether such Renewal is appropriate.

(c) The decision of the Association to implement or not to implement a Renewal shall be final and all SmartRight Participants shall be bound thereby.

5.3.7 Implementation of Renewal. The Association shall delay the implementation of any Renewal for a sufficient period of time to ensure a smooth transition from the old system to the Renewed system. During that period, all owners of SmartRight Products affected by the Renewal shall either be sent new SmartRight Smart Cards free of charge, or provided with the opportunity to acquire such cards free of charge at a location or locations established for that purpose, and any Certified Keys issued to Adopters who have not yet sold devices containing such keys, or to distributors or retailers of such devices who have not resold the devices to consumers, shall be replaced.

## 6. CONFIDENTIALITY.

6.1 Permitted Uses. A Party who receives Confidential Information (the “Receiving Party”) shall use any Confidential Information (and tangible embodiments of any of the foregoing) disclosed to it by the other Party (the “Disclosing Party”) solely for purposes of exercising its rights and performing its obligations under this Agreement.

6.2 No Circumvention. During the Confidentiality Period set forth in Section 6.9, below, Content Participant shall not itself nor assist others in producing any devices or software designed to circumvent the Compliance Rules or the effectiveness of the Specification.

6.3 Preservation of Confidentiality.

6.3.1 Highly Confidential Information. Content Participant shall maintain the confidentiality of Highly Confidential Information in the following manner:

(a) Content Participant shall employ procedures for safeguarding Highly Confidential Information at least as rigorous as Content Participant would employ

for its own most highly confidential information, such procedures to include, at a minimum: (1) maintaining on Content Participant's premises a secure location in which any and all Highly Confidential Information shall be stored; (2) such secure location shall be accessible only by authorized employees; (3) employees shall sign in and out each time such employees visit such secure location; and (4) when Highly Confidential Information is not in use, such information shall be stored in a locked safe at such secure location.

(b) Content Participant may disclose Highly Confidential Information only to the minimum possible number of regular employees of Content Participant: (1) who have an absolute need to know such Highly Confidential Information in order to enable Content Participant to implement SmartRight Technology in compliance with the Specification; and, (2) who are bound in writing by obligations of confidentiality sufficient to protect the Highly Confidential Information in accordance with the terms of this Agreement; and, (3) have made Parties who have entered into an agreement with the Authority consistent with the provisions hereof that authorizes such third party to receive such Highly Confidential Information

(c) Content Participant shall not make any copies of any Highly Confidential Information. Content Participant may request additional copies of such information and the Authority may in its sole discretion fulfill any such request.

**6.3.2 Other Confidential Information.** A Receiving Party may disclose Confidential Information of the Disclosing Party, other than Highly Confidential Information, only to employees and individuals retained as independent contractors subject to confidentiality obligations equivalent to those applicable to its own employees and contractors who have a reasonable need-to-know and are bound in writing by obligations of confidentiality sufficient to protect the Confidential Information in accordance with the terms of this Agreement. Each Receiving Party shall use the same degree of care, but no less than a reasonable degree of care, to avoid unauthorized disclosure or use of Confidential Information as such party employs with respect to its comparably important confidential information.

**6.4 Cooperation and Assistance.** Each Party receiving Confidential Information shall make all reasonable efforts to assist the Disclosing Party in relation to any claim, action, suit, proceeding, or litigation with respect to any improper or unauthorized use or disclosure of Confidential Information by any present or former employees of the Receiving Party or any third parties who have obtained Confidential Information from it.

**6.5 Contact Person.** Content Participant shall designate a single employee and an alternate employee who shall receive all Confidential Information and Highly Confidential Information (the "Content Participant Contact") disclosed by the Authority.

**6.6 Notification of Unauthorized Use or Disclosure.** Each Party shall notify the other Party in writing immediately upon discovery of any unauthorized use or disclosure of

Proprietary Information, and will cooperate with the Authority in every reasonable way to regain possession of Proprietary Information and prevent its further unauthorized use or disclosure.

6.7 Disclosure Required by Law. If a Receiving Party is required by law, regulation or order of a court or other Authority of competent jurisdiction to disclose Confidential Information, such Receiving Party shall promptly notify the Disclosing Party and shall make reasonable efforts to challenge the discloser or secure an appropriate protective order restricting the scope of use and disclosure of the Confidential Information.

6.8 Confidentiality Exceptions. The restrictions contained in this Section 6 shall not apply to information that the Receiving Party can demonstrate by documentary evidence: (i) has been generally known to the public through no breach of the Receiving Party's obligations for more than 120 days and the Disclosing Party has failed to institute reasonable measures to remove it from public availability or enjoin further public disclosure; (ii) was in the possession of the Receiving Party prior to its Disclosure by the Disclosing Party; (iii) was developed by the Receiving Party's employees (whether independently or jointly with others) without having access (whether directly or through any intermediaries) to such Confidential Information and without any breach of its obligations hereunder; or (iv) is or has been disclosed to the Receiving Party by a third party that had developed (whether independently or jointly with others) such information without any access (whether directly or through any intermediaries) to any Confidential Information and without any breach of any such third party's obligations to the Disclosing Party. Notwithstanding the foregoing, any Certified Keys provided to the Content Participant shall not lose their status as Highly Confidential Information.

6.9 Confidentiality Period. The confidentiality obligations set forth herein shall continue until five (5) years after the last commercial use of SmartRight Technology by the Authority or any Fellow Content Participant.

7. **COMPLIANCE WITH EXPORT LAWS.**

7.1 Content Participant will comply with all applicable rules and regulations of the United States, Japan, Member States of the European Union, and other countries and jurisdictions, including those relating to the export or re-export of commodities, software and technical data insofar as they relate to the activities under this Agreement. Content Participant is aware that commodities, software and technical data provided under this Agreement may be and/or are subject to restrictions under the export control laws and regulations of the United States, Japan, Member States of the European Union and other countries and jurisdictions, as applicable, including but not limited to the U.S. Export Administration Act and the U.S. Export Administration Regulations, any relevant and applicable European Union rules and procedures (including rules and procedures of the Member States of the European Union), and the Japanese Foreign Exchange and Foreign Trade Law, and shall obtain any approval required under such laws and regulations whenever it is necessary for such export or re-export.

8. **TERM/TERMINATION.**

8.1 Termination. This Agreement shall be effective as of the Effective Date and shall remain in full force and effect until terminated in accordance with the terms of this Section 8.

8.1.1 Termination by Content Participant. Content Participant may terminate this Agreement at any time upon ninety (90) days notice to Authority.

8.1.2 Termination by Authority. Authority may terminate this Agreement (a) for convenience at any time after the tenth anniversary of the Effective Date upon six (6) months notice to Content Participant; (b) at any time upon six (6) months notice to Content Participant if Authority determines, in its sole discretion, that it is not commercially reasonable to carry on the business of licensing SmartRight; or (c) upon notice to Content Participant if the use of SmartRight is enjoined, or Authority determines, in its sole discretion, that it may be enjoined, due to an alleged infringement of a third-party intellectual property right. Without limiting the foregoing, in the event that Authority provides notice of termination to Content Participant pursuant to Section 8.1.2(a) or 8.1.2(b), Authority shall, upon request of Content Participant, meet with Content Participant, reasonably promptly after such notice, to discuss in good faith possible approaches to enable the continued licensing of SmartRight; provided that if a majority of Major Content Participants are willing, and agree in a written agreement satisfactory to Authority at its reasonable discretion; to (i) assume financial responsibility for the operation, maintenance and liabilities of the Key Generator, (ii) provide fair and reasonable compensation to Authority for the continued licensing by Authority of the intellectual property licensed to Content Providers and Adopters under this Agreement and all other Operative Agreements and for the administration of such licenses, Authority will not terminate this Agreement or the other Operative Agreements for the reasons specified in Section 8.1.2(a) or 8.1.2(b). In the event of termination pursuant to Section 8.1.2(a), Authority shall refund to Content Participant a percentage of the Administration Fee allocable to the portion of the then-current Contract Year following such termination, based on a pro-rata allocation of such Administration Fee. In the event of termination pursuant to Section 8.1.2(b) or 8.1.2(c), Authority shall refund to Content Participant the Administration Fee paid by Content Participant for the then-current Contract Year.

8.1.3 Breach. In the event that either Party (a) materially breaches any of its obligations hereunder, which breach is not cured, or not capable of cure, within thirty (30) days after notice is given to the breaching Party specifying the breach; or (b) repeatedly breaches any of its obligations hereunder and fails to cure and cease committing such repeated breaches within thirty (30) days after being given notice specifying the breaches, then the Party not in breach may, by giving notice thereof to the breaching Party, terminate this Agreement, upon the expiration of a thirty (30) day period beginning on the date of such notice of termination, or in the event of a material breach that is not capable of cure within such thirty (30) day period, upon such notice of termination.

8.2 Effect of Termination. Upon termination of this Agreement, any licenses granted to Content Participant hereunder immediately shall terminate. Within ninety (90) days (or in the case of termination by Authority pursuant to Section 8.1.3, thirty (30) days) after termination of this Agreement, Content Participant shall return all Confidential Information to Authority or, at Authority's option, destroy all such information in its possession, retaining no copies thereof, and certify such destruction in writing to Authority. Content Participant shall pay any outstanding Administration Fees within thirty (30) days of termination of this Agreement.

8.3 Survival. The terms of Sections 2.2, 2.3, 2.4, 6, 8.2, 10, 11, 12 and this Section 8.3 shall survive any termination of this Agreement.

9. **REPRESENTATIONS OF CONTENT PARTICIPANT AND AUTHORITY.**

9.1 Compliance With Laws. Content Participant and Authority each represent and warrant that they shall comply with all applicable governmental regulations, laws and orders pertaining to SmartRight, including but not limited to with respect to export requirements pursuant to Section 7.

10. **DISCLAIMER AND LIMITATION OF LIABILITY.**

10.1 The terms of this Section 10 limit the ability of Content Participant to recover damages from Authority or any Affiliate thereof. The terms of this Section 10 are an essential part of the bargain, without which Authority would not be willing to enter into this Agreement.

10.2 Disclaimer. ALL INFORMATION, MATERIALS AND TECHNOLOGY, INCLUDING BUT NOT LIMITED TO SMARTRIGHT, THE SMARTRIGHT SPECIFICATION AND DEVICE KEYS ARE PROVIDED "AS IS." AUTHORITY, KEY GENERATOR AND THEIR RESPECTIVE AFFILIATES MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND EXPRESSLY DISCLAIM IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION THAT MIGHT ARISE FROM ANY ACTIVITIES OR INFORMATION DISCLOSURES RELATING TO THIS AGREEMENT, ANY OTHER AGREEMENT OR ANY OTHER ACTIVITY OF THE AUTHORITY. THE AUTHORITY, KEY GENERATOR AND THEIR RESPECTIVE AFFILIATES FURTHER DISCLAIM ANY WARRANTY THAT SMARTRIGHT, THE SMARTRIGHT SPECIFICATION, OR ANY IMPLEMENTATION OF THE SMARTRIGHT SPECIFICATION, IN EACH CASE IN WHOLE OR IN PART, WILL BE FREE FROM INFRINGEMENT OF ANY INTELLECTUAL PROPERTY OR PROPRIETARY RIGHTS. WITHOUT LIMITING THE FOREGOING, AUTHORITY, KEY GENERATOR AND THEIR RESPECTIVE AFFILIATES DO NOT REPRESENT OR WARRANT THAT SMARTRIGHT IS IMMUNE TO HACKING, CODE-BREAKING, PIRACY OR OTHER EFFORTS TO CIRCUMVENT SMARTRIGHT.

10.3 Limitation of Liability. NONE OF AUTHORITY, KEY GENERATOR, AFFILIATES OF ANY OF THE FOREGOING, NOR ANY OF THEIR RESPECTIVE DIRECTORS, OFFICERS, AGENTS, MEMBERS, REPRESENTATIVES, EQUIVALENT CORPORATE OFFICIALS, OR EMPLOYEES ACTING IN THEIR CAPACITIES AS SUCH (COLLECTIVELY, THE "AFFECTED PARTIES") SHALL BE LIABLE TO CONTENT PARTICIPANT, NOR SHALL CONTENT PARTICIPANT BE LIABLE TO THE AFFECTED PARTIES, FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR PUNITIVE DAMAGES ARISING OUT OF ANY CAUSE OF ACTION RELATING TO THIS AGREEMENT, OR BASED ON THE MAKING, USING, SELLING, OFFERING FOR SALE OR IMPORTING OF ANY PRODUCTS THAT IMPLEMENT SMARTRIGHT OR ANY PORTION OF THE SMARTRIGHT SPECIFICATION, WHETHER UNDER THEORY OF CONTRACT, TORT, INDEMNITY, PRODUCT LIABILITY OR OTHERWISE. WITHOUT LIMITING THE FOREGOING, IN NO EVENT WILL THE AFFECTED PARTIES' AGGREGATE LIABILITY TO CONTENT PARTICIPANT ARISING OUT OF ANY AND ALL CAUSES OF ACTION RELATING TO THIS AGREEMENT, OR BASED ON THE MAKING, USING, SELLING, OFFERING FOR SALE OR IMPORTING OF ANY PRODUCTS THAT IMPLEMENT SMARTRIGHT OR ANY PORTION OF THE SMARTRIGHT SPECIFICATION, WHETHER UNDER THEORY OF CONTRACT, TORT, INDEMNITY, PRODUCT LIABILITY OR OTHERWISE, EXCEED THE ANNUAL FEE ACTUALLY RECEIVED BY AUTHORITY FROM CONTENT PARTICIPANT UNDER THIS AGREEMENT DURING THE THEN-PRECEDING ONE (1) YEAR PERIOD.

11. **REMEDIES.**

11.1 Equitable Relief. Content Participant and Authority acknowledge and agree that due to the unique nature of certain provisions hereof and the lasting effect of and harm from a breach of such provisions, in the event that Content Participant breaches its obligations under the Confidentiality Agreement, Authority shall be entitled to specific performance or other temporary, preliminary, or permanent injunctive or equitable relief including corrective actions appropriate to the circumstances for the enforcement of any such obligation and prevention of future breaches. In the event that Content Participant willfully breaches, or engages in a pattern or practice of breaching, its obligations hereunder, it shall be liable for Authority's attorneys' fees and expenses incurred in connection with any enforcement action brought by Authority in which Authority is the prevailing party.

12. **MISCELLANEOUS.**

12.1 Ownership. All Licensed Technology and Confidential Information provided by Authority to Content Participant hereunder shall remain the property of Authority.

12.2 Entire Agreement. This Agreement, including the exhibits hereto, constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes all oral or written agreements, either entered prior to or contemporaneously

with this Agreement. This Agreement may not be modified except by written agreement of both Parties.

12.3 Assignment. The rights and licenses granted under this Agreement to Content Participant are personal to Content Participant and shall not be assigned or otherwise transferred except: (a) with the written approval of Authority; (b) to a corporation controlling, controlled by or under common control with Content Participant; (c) or to the purchaser of all or substantially all of the outstanding capital stock or assets and obligations of Content Participant or the surviving entity in a merger, reorganization, or other business combination involving Content Participant; provided notice of such assignment has been provided in advance to Authority and the surviving or acquiring company has agreed in writing to be bound by the terms of this Agreement. Subject to the limitations set forth in this Agreement, this Agreement shall inure to the benefit of and be binding upon the Parties, their successors and permitted assigns. Authority may assign or transfer this Agreement to any Person that agrees to assume Authority's obligations hereunder, and Authority shall provide Content Participant with notice of such assignment or transfer.

12.4 Presumptions. In construing the terms of this Agreement, no presumption shall operate in either Party's favor as a result of its counsel's role in drafting the terms or provisions hereof.

12.5 Governing Law; Jurisdiction. THIS AGREEMENT SHALL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF NEW YORK APPLICABLE TO AGREEMENTS MADE AND TO BE PERFORMED ENTIRELY IN SUCH STATE, AND WITH THE LAWS OF THE UNITED STATES AS WOULD BE CONSTRUED BY A COURT SITTING IN THE SOUTHERN DISTRICT OF NEW YORK.

12.5.1 IN CONNECTION WITH ANY LITIGATION BETWEEN THE PARTIES HERETO ARISING OUT OF OR RELATING TO THIS AGREEMENT, EACH PARTY IRREVOCABLY CONSENTS TO: (a) THE NON-EXCLUSIVE JURISDICTION AND VENUE IN THE FEDERAL AND STATE COURTS LOCATED IN THE COUNTY OF NEW YORK, NEW YORK, AND IN THE FEDERAL AND STATE COURTS LOCATED IN LOS ANGELES COUNTY OF CALIFORNIA; AND (b) THE SERVICE OF PROCESS OF SUCH COURTS IN ANY MATTER RELATING TO THIS AGREEMENT BY PERSONAL DELIVERY OR BY MAILING OF PROCESS BY REGISTERED OR CERTIFIED MAIL, POSTAGE PREPAID, AT THE ADDRESSES SPECIFIED IN THIS AGREEMENT, OR TO THE AGENT TO BE APPOINTED PURSUANT TO SECTION 12.5.3.

12.5.2 EACH PARTY WAIVES ANY OBJECTION TO THE JURISDICTION, PROCESS, AND VENUE OF ANY SUCH COURTS, AND TO THE EFFECTIVENESS, EXECUTION, AND ENFORCEMENT OF ANY ORDER OR JUDGMENT (INCLUDING, BUT NOT LIMITED TO, A DEFAULT JUDGMENT) OF SUCH COURTS PERTAINING TO THIS AGREEMENT, TO



THE MAXIMUM EXTENT PERMITTED BY THE LAW OF THE PLACE WHERE ENFORCEMENT OR EXECUTION OF ANY SUCH ORDER OR JUDGMENT MAY BE SOUGHT AND BY THE LAW OF ANY PLACE WHOSE LAW MAY BE CLAIMED TO BE APPLICABLE REGARDING THE EFFECTIVENESS, ENFORCEMENT, OR EXECUTION OF SUCH ORDER OR JUDGMENT, INCLUDING PLACES OUTSIDE OF THE STATES OF NEW YORK, CALIFORNIA, AND THE UNITED STATES.

12.5.3 IF CONTENT PARTICIPANT DOES NOT HAVE A PLACE OF BUSINESS IN AT LEAST ONE OF THE STATES OF NEW YORK OR CALIFORNIA, IT SHALL APPOINT AN AGENT IN AT LEAST ONE SUCH STATE FOR ACCEPTANCE OF SERVICE OF PROCESS PROVIDED FOR UNDER THIS AGREEMENT AND SHALL NOTIFY AUTHORITY OF THE IDENTITY AND ADDRESS OF SUCH AGENT WITHIN THIRTY (30) DAYS AFTER THE EFFECTIVE DATE.

12.6 Notice. Unless otherwise specified in this Agreement, all notices to be provided pursuant to this Agreement shall be given in writing and shall be effective when either served by personal delivery or upon receipt via certified mail, return receipt requested, postage prepaid, overnight courier service or sent by facsimile transmission with hard copy confirmation sent by certified mail, in each case to the party at the addresses set out on the signature page hereof.

12.7 Severability; Waiver. In the event that any part or parts of this Agreement is (are) judicially declared to be invalid, unenforceable, or void, the Parties agree that such part or parts so held to be invalid, unenforceable, or void shall be reformed by the entity having jurisdiction thereover without further action by the Parties hereto and only to the extent necessary to make such part or parts valid and enforceable. A waiver by either of the Parties hereto of any of the covenants to be performed by the other Party or any breach of this Agreement shall not be effective unless made in writing and signed by the waiving Party and shall not be construed to be a waiver of any succeeding breach thereof or of any covenant herein contained.

12.8 Headings and Captions. Section headings in this Agreement are for convenience only and shall not affect the interpretation of any provision of this Agreement.

12.9 Counterparts. This Agreement may be executed in any number of counterparts, each of which shall be an original, but all of which together shall constitute one instrument.

12.10 Currency. All fees payable to Authority hereunder shall be paid to Authority in United States dollars by wire transfer or such other means as Authority may reasonably specify.

## SmartRight Content Participant Agreement

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the date first above written.

**SmartRight Licensing Authority, LLC:**

**Content Participant:**

By: \_\_\_\_\_

By: \_\_\_\_\_

Name: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Date: \_\_\_\_\_

Addresses for notices

**SmartRight Licensing Authority, L.L.C.:**

**Content Participant:**

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

EXHIBIT A

ANNUAL FEES

US \$30,000

EXHIBIT B

FORM ADOPTER AGREEMENT

[See Adopter Agreement Submitted to the FCC]

**CERTIFICATE OF SERVICE**

The undersigned hereby certifies that true and correct copies of the foregoing were served on the following individuals on April 16, 2004, by first-class mail, postage pre-paid:

Jon A. Baumgarten  
Proskauer Rose LLP  
1233 Twentieth Street, N.W.  
Suite 800  
Washington, D.C. 20036

Bruce Boyden  
Proskauer Rose LLP  
1233 Twentieth Street, N.W.  
Suite 800  
Washington, D.C. 20036



---

David H. Arland